[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00
G11B 27/00 G11B 20/10

[12] 发明专利申请公开说明书

[21] 申请号 01804335.6

[43] 公开日 2003 年 2 月 12 日

[11] 公开号 CN 1397123A

[22] 申请日 2001.10.19 [21] 申请号 01804335.6
[30] 优先权
[32] 2000.10.20 [33] JP [31] 320804/2000
[86] 国际申请 PCT/JP01/09182 2001.10.19
[87] 国际公布 WO02/33880 日 2002.4.25
[85] 进入国家阶段日期 2002.7.30
[71] 申请人 索尼公司
地址 日本东京都
[72] 发明人 秋下彻 石桥义人 吉野贤治
白井太三

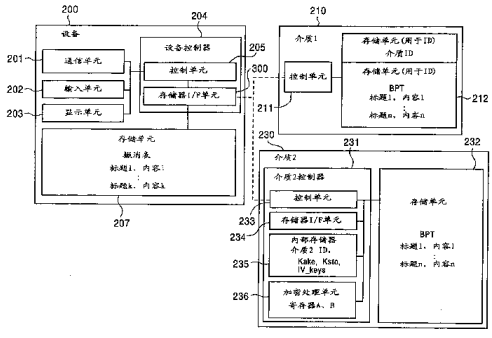
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森

权利要求书 11 页 说明书 61 页 附图 57 页

[54] 发明名称 数据再现/记录设备和方法,和表格更新方法

[57] 摘要

把属于不同类别的介质和内容两者的标识符存储在一个撤消表中，并且还设置版本信息。 可以把该表格建立在存储器接口中，在安装介质时和在再现内容时可以不断使用它。 当读出内容时，核实设备保存的撤消表的版本，在保存的撤消表的版本较旧的情况下，取消内容的读出。 此外，通过在安装介质时与介质标识符进行核对，和在使用内容时与内容标识符进行核对，排除伪内容和伪介质。



ISSN1008-4274

1. 一种对存储在数据存储装置中的内容执行再现处理的数据再现设备，包括:

内部存储器，用于存储撤消表，所述撤消表是存储作为禁止处理对象的至少一个数据存储装置或内容的标识符的表格，所述表格含有指示表格的新旧程度的版本信息；和

控制器，用于执行存储在作为再现对象的内容的标题信息中的有效撤消表版本与存储在所述内部存储器中的撤消表的版本之间的比较处理，和在确认存储在所述内部存储器中的撤消表的版本不旧于设置在作为再现对象的所述内容的标题信息中的版本的条件下，进行与作为再现对象的所述内容的再现同时进行的处理。

2. 根据权利要求 1 所述的数据再现设备，其中，所述控制器含有对存储在所述内部存储器中的撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符进行比较处理，作为与所述再现同时进行的处理的结构；和

具有在存储在撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符在所述比较处理中相匹配的情况下，执行取消数据再现的处理的结构。

3. 根据权利要求 1 所述的数据再现设备，其中，所述控制器含有执行对所述数据存储装置的存取的存储器接口、和执行对所述存储器接口的控制的控制单元；和

其中，所述存储器接口具有根据来自所述控制单元的数据再现请求命令，对存储在作为再现对象的内容的标题信息中的有效撤消表的版本与存储在所述内部存储器中的撤消表的版本进行比较处理的结构。

4. 根据权利要求 1 所述的数据再现设备，所述控制器含有对从外部接收的更新撤消表的版本与已经存储在所述内部存储器中的撤消表的版本进行比较处理，和在确认存储在所述内部存储器中撤消表的版本比所述更新撤消表的版本新的条件下，通过所述更新撤消表执行撤消表的更新处理的结构。

5. 根据权利要求 4 所述的数据再现设备，其中，所述控制器含有进行基于数据完整性检验值（ICV）的、与从外部接收的更新撤消表有关的数据

窜改检验，和根据没有数据被窜改的判断，通过所述更新撤消表执行撤消表的更新处理的结构。

6. 一种对要存储在数据存储装置中的内容执行记录处理的数据记录设备，包括:

内部存储器，用于存储撤消表，所述撤消表是存储作为禁止处理对象的至少一个数据存储装置或内容的标识符的表格，所述表格含有指示表格的新旧程度的版本信息；和

控制器，用于执行把指定不参考撤消表进行再现处理的设置值设置成要存储在作为记录对象的内容的标题信息中的有效撤消表版本的处理，和对所述数据存储装置执行内容存储处理。

7. 根据权利要求 6 所述的数据再现设备，其中，所述控制器含有执行对所述数据存储装置的存取的存储器接口、和执行对所述存储器接口的控制的控制单元;

其中，所述存储器接口具有根据来自所述控制单元的伴随着数据记录的标题信息生成命令，执行把要存储在作为记录对象的内容的标题信息中的有效撤消表的版本设置成能够不参考撤消表进行再现的设置值的处理的结构。

8. 根据权利要求 6 所述的数据再现设备，其中，所述控制器含有对从外部接收的更新撤消表的版本与已经存储在所述内部存储器中的撤消表的版本进行比较处理，和在确认存储在所述内部存储器中撤消表的版本比所述更新撤消表的版本新的条件下，通过所述更新撤消表执行撤消表的更新处理的结构。

9. 根据权利要求 8 所述的数据再现设备，其中，所述控制器含有进行基于数据完整性检验值（ICV）的、与从外部接收的更新撤消表有关的数据窜改检验，和根据没有数据被窜改的判断，通过所述更新撤消表执行撤消表的更新处理的结构。

10. 一种用于对存储在数据存储装置中的数据执行再现处理的数据再现设备的数据再现方法，所述方法包括:

比较步骤，对存储在作为再现对象的内容的标题信息中的有效撤消表版本与存储在所述数据再现设备的内部存储器中的撤消表的版本进行比较处理；和

再现相关处理执行步骤，在确认存储在所述内部存储器中的撤消表的版

本不旧于设置在作为再现对象的所述内容的标题信息中的版本的条件下，进行与作为再现对象的所述内容的再现同时进行的处理。

11. 根据权利要求 10 所述的数据再现方法，其中，所述再现相关处理执行步骤包含对存储在所述内部存储器中的撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符进行比较处理的步骤；和

在存储在所述撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符在所述比较处理中相匹配的情况下，执行取消数据再现的处理的步骤。

12. 根据权利要求 10 所述的数据再现方法，其中，所述数据再现设备含有执行对所述数据存储装置的存取的存储器接口、和执行对所述存储器接口的控制的控制单元，

所述数据再现方法还包括:

把数据再现请求命令从所述控制单元发送到所述存储器接口的步骤；和

根据所述数据再现请求命令在所述存储器接口上的接收，对存储在作为再现对象的内容的标题信息中的有效撤消表的版本与存储在所述内部存储器中的撤消表的版本进行比较处理的步骤。

13. 一种对要存储在数据存储装置中的内容执行记录处理的数据记录方法包括:

执行把指定不参考撤消表进行再现处理的设置值设置成要存储在作为记录对象的内容的标题信息中的有效撤消表版本的处理的步骤；和

对所述数据存储装置执行内容存储处理的步骤。

14. 一种用于数据处理设备的表格更新方法，把撤消表存储在内部存储器中，所述撤消表是存储作为禁止处理对象的至少一个数据存储装置或内容的标识符的表格，所述表格含有指示表格的新旧程度的版本信息;

其中，执行从外部接收的更新撤消表的版本与已经存储在所述内部存储器中的撤消表的版本之间的比较处理，和在确认存储在所述内部存储器中撤消表的版本比所述更新撤消表的版本新的条件下，通过所述更新撤消表执行撤消表的更新处理。

15. 根据权利要求 14 所述的表格更新方法，还包括:

进行基于数据完整性检验值（ICV）的、与从外部接收的更新撤消表有

关的数据窜改检验的步骤;

其中，根据没有数据被窜改的判断，通过所述更新撤消表执行撤消表的更新处理。

16. 一种为对存储在数据存储装置中的数据执行再现处理的数据再现设备提供使数据再现处理可以在计算机系统上得以执行的计算机程序的程序提供介质，其中，所述计算机程序包括:

比较步骤，对存储在作为再现对象的内容的标题信息中的有效撤消表版本与存储在所述数据再现设备的内部存储器中的撤消表的版本进行比较处理; 和

再现相关处理执行步骤，在确认存储在所述内部存储器中的撤消表的版本不旧于设置在作为再现对象的所述内容的标题信息中的版本的条件下，进行与作为再现对象的所述内容的再现同时进行的处理。

17. 一种对存储在数据存储装置中的内容执行再现处理的数据再现设备;

其中，所述数据再现设备具有把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中，和在存储器接口内的相继不同处理中，以可参考状态保存撤消表的结构。

18. 根据权利要求 17 所述的数据再现设备，还包括对撤消表设置命令执行发送处理，作为在启动时的处理的控制单元，所述撤消表设置命令是与所述存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令;

其中，所述存储器接口具有响应所述撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在所述存储器接口内进行参考处理的结构。

19. 根据权利要求 17 所述的数据再现设备，其中，所述存储器接口具有进行与读入所述存储器接口的撤消表有关的、基于数据完整性检验值（ICV）的数据窜改检验，和在判断没有数据被窜改的条件下，执行能够在所述存储器接口内进行参考处理的撤消表设置处理的结构。

20. 根据权利要求 17 所述的数据再现设备，其中，所述存储器接口具有从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在

所述接收的数据存储装置标识符与列在设置在所述存储器接口中的撤消表中的标识符进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

21. 根据权利要求 17 所述的数据再现设备，所述存储器接口具有从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在设置在所述存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

22. 根据权利要求 17 所述的数据再现设备，其中，所述撤消表具有含有作为禁止处理对象的数据存储装置和作为禁止处理对象的内容两者的标识符数据的结构。

23. 一种对要存储在数据存储装置中的内容执行记录处理的数据记录设备;

其中，所述数据记录设备具有把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中，和在存储器接口的相继不同处理中，以可参考状态保存撤消表的结构。

24. 根据权利要求 23 所述的数据再现设备，还包括对撤消表设置命令执行发送处理，作为在启动时的处理的控制单元，所述撤消表设置命令是与所述存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令;

其中，所述存储器接口具有所述响应撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在所述存储器接口内进行参考处理的结构。

25. 根据权利要求 23 所述的数据再现设备，其中，所述存储器接口具有进行与读入所述存储器接口的撤消表有关的、基于数据完整性检验值（ICV）的数据窜改检验，和在判断没有数据被窜改的条件下，执行能够在所述存储器接口内进行参考处理的撤消表设置处理的结构。

26. 根据权利要求 23 所述的数据再现设备，其中，所述存储器接口具有从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在所述接收的数据存储装置标识符与列在设置在所述存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理

的结构。

27. 根据权利要求 23 所述的数据再现设备，其中，所述撤消表具有含有与作为禁止处理对象的数据存储装置和作为禁止处理对象的内容两者有关的标识符数据的结构。

28. 一种对存储在数据存储装置中的内容执行再现处理的数据再现方法，所述方法包括:

把保存作为禁止处理对象的至少一个数据存储装置或内容的撤消表标识符数据读入对数据存储装置进行存取的存储器接口中的步骤;

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤;和

参考设置在存储器接口中的撤消表，判断数据再现处理是允许的还是不允许的步骤。

29. 根据权利要求 28 所述的数据再现方法，还包括:

对撤消表设置命令执行发送处理，作为在启动时的处理的步骤，所述撤消表设置命令是来自控制单元的、与对数据存储装置进行存取的存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令; 和

在所述存储器接口上，响应所述撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在存储器接口内进行参考处理的步骤。

30. 根据权利要求 28 所述的数据再现方法，其中，还进行与读入存储器接口的撤消表有关的、基于数据完整性检验值（ICV）的数据窜改检验，和其中，在判断没有数据被窜改的条件下，执行能够在所述存储器接口内进行参考处理的撤消表设置处理。

31. 根据权利要求 28 所述的数据再现方法，还包括: 在所述存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在所述接收的数据存储装置标识符与列在设置在所述存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤。

32. 根据权利要求 28 所述的数据再现方法，还包括: 在所述存储器接口上，从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内

容的标识符，在获取的内容标识符与列在设置在所述存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤。

33. 一种对要存储在数据存储装置中的内容执行记录处理的数据记录方法，所述方法包括:

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤;

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤;和

参考设置在存储器接口中的撤消表，判断数据记录处理是允许的还是不允许的步骤。

34. 根据权利要求 33 所述的数据再现方法，还包括:

对撤消表设置命令执行发送处理，作为在启动时的处理的步骤，所述撤消表设置命令是来自控制单元的、与对数据存储装置进行存取的所述存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令;

在所述存储器接口上，响应所述撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在所述存储器接口内进行参考处理的步骤；和

参考设置在存储器接口中的撤消表，判断数据记录处理是允许的还是不允许的步骤。

35. 根据权利要求 33 所述的数据记录方法，其中，还进行与读入所述存储器接口的撤消表有关的、基于数据完整性检验值（ICV）的数据窜改检验，和在判断没有数据被窜改的条件下，执行能够在所述存储器接口内进行参考处理的撤消表设置处理。

36. 根据权利要求 33 所述的数据记录方法，还包括：在所述存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在所述接收的数据存储装置标识符与列在设置在所述存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据记录处理的步骤。

37. 一种为了对存储在数据存储装置中的内容执行再现处理而提供使再

现处理可以在计算机系统上得以执行的计算机程序的程序提供介质，所述计算机程序包括:

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤;

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤;和

参考设置在所述存储器接口中的撤消表，判断数据再现处理是允许的还是不允许的步骤。

38. 一种为了对要存储在数据存储装置中的内容执行记录处理而提供使记录处理可以在计算机系统上得以执行的计算机程序的程序提供介质，所述计算机程序包括:

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤;

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤;和

参考设置在所述存储器接口中的撤消表，判断数据记录处理是允许的还是不允许的步骤。

39. 一种对存储在数据存储装置的内容执行再现处理的数据再现设备，所述数据再现设备含有:

执行对所述数据存储装置的存取的存储器接口，和执行对所述存储器接口的控制的控制单元;

所述存储器接口含有内部存储器，用于存储保存与作为禁止处理对象的数据存储装置和内容的每一个有关的标识符数据的撤消表;

其中，所述存储器接口含有从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构; 和

其中，从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

40. 根据权利要求 39 所述的数据再现设备，含有所述存储器接口根据

来自所述控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理的结构。

41. 根据权利要求 39 所述的数据再现设备，含有所述存储器接口根据来自所述控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在所述相互验证处理期间接收数据存储装置标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理的结构。

42. 根据权利要求 39 所述的数据再现设备，含有所述存储器接口根据来自所述控制单元的数据再现请求命令，获取存储在要再现的内容的标题信息中的内容标识符，和在所述获取的内容标识符与列在所述撤消表中的标识符之间执行核对处理的结构。

43. 根据权利要求 39 所述的数据再现设备，其中，所述存储器接口含有进行基于数据完整性检验值（ICV）的，与从外部接收的更新撤消表有关的数据窜改检验，从而判断没有数据被窜改的结构；和

其中，执行从外部接收的更新撤消表的版本与已经存储在所述内部存储器中的撤消表的版本之间的比较处理，和在确认存储在所述内部存储器中的撤消表的版本比所述更新撤消表新的条件下，通过所述更新撤消表执行撤消表的更新处理。

44. 一种对要存储在数据存储装置的内容执行记录处理的数据记录设备，所述数据记录设备含有：

执行对所述数据存储装置的存取的存储器接口，和执行对所述存储器接口的控制的控制单元；

所述存储器接口含有内部存储器，用于存储保存与作为禁止处理对象的数据存储装置和内容的每一个有关的标识符数据的撤消表；

其中，所述存储器接口含有接收作为记录数据的对象的数据存储装置标识符，在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据记录处理的结构。

45. 根据权利要求 44 所述的数据记录设备，含有所述存储器接口根据来自所述控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间

执行核对处理的结构。

46. 根据权利要求 44 所述的数据记录设备，含有所述存储器接口根据来自所述控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在所述相互验证处理期间接收数据存储装置标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理的结构。

47. 一种对存储在数据存储装置的内容执行再现处理的数据再现方法;

其中，在执行对所述数据存储装置的存取的存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理；和

其中，从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在所述获取的内容标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理。

48. 根据权利要求 47 所述的数据再现方法，其中，在所述存储器接口上，根据来自控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理。

49. 根据权利要求 47 所述的数据再现方法，其中，在所述存储器接口上，根据来自控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在所述相互验证处理期间接收数据存储装置标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理。

50. 根据权利要求 47 所述的数据再现方法，其中，在所述存储器接口上，根据来自控制单元的数据再现请求命令，获取存储在要再现的内容的标题信息中的内容标识符，和在所述获取的内容标识符与列在所述撤消表中的标识符之间执行核对处理。

51. 一种对要存储在数据存储装置的内容执行记录处理的数据记录方法;

其中，在执行对所述数据存储装置的存取的存储器接口上，接收作为记录数据的对象的所述数据存储装置标识符，在所述接收的数据存储装置标识

符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，执行取消数据记录的处理；

52. 根据权利要求 51 所述的数据记录方法，其中，在所述存储器接口上，根据来自控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理。

53. 根据权利要求 51 所述的数据记录方法，其中，在所述存储器接口上，根据来自所述控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在所述相互验证处理期间接收数据存储装置标识符，和在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间执行核对处理。

54. 一种为了对存储在数据存储装置中的内容执行再现处理而提供使再现处理可以在计算机系统上得以执行的计算机程序的程序提供介质，所述计算机程序包括：

在执行对所述数据存储装置的存取的存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤；和

从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在所述获取的内容标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤。

55. 一种为了对要存储在数据存储装置中的内容执行记录处理而提供使记录处理可以在计算机系统上得以执行的计算机程序的程序提供介质，所述计算机程序包括：

在执行对所述数据存储装置的存取的存储器接口上，接收作为记录数据的对象的所述数据存储装置的标识符，在所述接收的数据存储装置标识符与列在所述撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据记录处理的步骤。

数据再现／记录设备和方法，和表格更新方法

技术领域

本发明涉及数据再现设备和数据记录设备、数据再现方法和数据记录方法、表格更新方法、和程序提供介质。本发明尤其涉及能够对为了撤消未授权介质和未授权内容等而生成的撤消表进行版本管理，并且能够有效参考和使用撤消表的数据再现设备和数据记录设备、数据再现方法和数据记录方法、表格更新方法、和程序提供介质。

背景技术

近年来因特网的迅速普及，以及移动式小型播放器和游戏设备等的广泛使用导致了音乐数据、游戏程序和图像数据之类的各种软数据（下文称之为内容）通过因特网之类的网络或 DVD（数字视频盘）、CD（光盘）和存储卡之类的记录介质的分配迅速增加。通过用户拥有的 PC（个人计算机）、专用再现设备、或游戏设备从网络接收这些分配内容，并且将其存储在记录介质中，或者，将存储卡、CD 和 DVD 之类存储内容的记录介质安装到专用再现设备或游戏设备上，这些分配内容可以经受内容播放处理或程序执行处理。

最近常用作内容记录设备的设备是闪速存储器。闪速存储器是一种被称为 EEPROM（电可擦除可编程只读存储器）的、可电重写的非易失性存储器。传统 EEPROM 用两个晶体管构成一个位，因此，一个位所占据的空间较大，在提高集成度方面受到了限制，但是，通过对所有位进行块擦除（block erasing），闪速存储器能够让一个位用一个晶体管来实现。因此，闪速存储器有望取代磁盘和光盘之类的记录介质。

其中把闪速存储器做成可与数据记录／再现设备分开的存储卡也是已知的。使用这样的存储卡使得数字音频记录／再现设备可以利用存储卡来取代 CD（光盘：注册商标）和 MD（小型盘：注册商标）之类的盘状介质而得以实现。

在个人计算机（PC）和再现设备等把闪速存储器用作内容存储设备的情况下，称为 FAT（文件分配表）的文件管理系统通常用作存取信息表。借助

于 FAT 系统，一旦定义了必要的文件，就从文件的头部开始依次设置其中必要的参数。因此，可以使文件大小是可变的，和一个文件可以由一个或多个管理单位（扇区或簇等）构成。与管理单位相关的项目被写入称为 FAT 的表中。这个 FAT 系统使文件与记录介质的物理特性无关地易于构造。因此，FAT 系统不仅可以与软盘和硬盘一起应用，而且可以与磁光盘一起应用。此外，FAT 系统还可以与上述存储卡一起应用。

诸如音乐数据、图像数据和程序之类的各种内容数据通过来自再现设备、游戏设备、或诸如 PC 之类用作再现设备的信息设备主单元的用户指令，或通过相连的输入装置的用户指令，根据上述 FAT，从，例如，上述闪速存储器中取出，然后通过信息设备主单元，或相连的显示器、扬声器等再现。

并且，对于游戏程序、音乐数据和图像数据之类的许多软件内容，一般来说，创作者和分配者拥有分配的权利。因此，就这些内容的分配来说，习以为常的做法是，对软件的使用作某些使用限制，即，只允许有效用户使用软件，和采取措施以杜绝未经允许的复制等，即，在结构上要考虑保密性问题。

对用户实现使用限制的一种技术是对分配内容进行加密处理。也就是说，通过，例如，因特网分配已经加密了的、诸如音频数据、图像数据和游戏程序之类的各种内容，而把解密分配的加密内容的工具，即，解密密钥只提供给被识别为有效用户的个体。

加密数据可以通过基于预定过程的解密处理恢复成可用的解密数据（明文）。把加密密钥用于这样的加密处理和把解密密钥用于这样的解密处理的加密和解密方法按照惯例，是众所周知的。

人们已经提议把撤消表用作内容记录／再现设备中，撤消未授权介质和未授权内容的方法。对内容进行记录和再现的设备在，例如，再现内容时，对存储内容的内容标识符和列在撤消表中的内容标识符进行核对，在发现标识符相匹配的情况下，由于内容是未授权的，进行取消再现处理的处理，从而，使未授权内容的使用能够得以撤消。

但是，还存在着通过窜改撤消表，或者进行诸如用未授权撤消表取代发送到设备的表格之类的处理，进行使未授权内容等能够得以再现的处理的可能性。例如，可以设想一下拥有无效的未授权介质或内容的攻击者不去更新其中未授权介质或内容并非无效的旧撤消表的情况。这将使未授权介质能够

得以使用和被认为无效的未授权内容能够被读取。

此外，还进行了把撤消表存储在，例如，记录／再现设备的内部存储器中的处理，和执行了在必要的时候和在要使用的时候从内部存储器中取出表格的参考处理。例如，设备重复执行如下那样的处理，例如，在再现内容的情况下，通过从内部存储器中读取存储未授权内容标识符的撤消表，执行参考处理，和在把目标对准撤消未授权介质的处理的情况下，通过从内部存储器中读取存储未授权介质标识符的撤消表，执行参考处理。每当安装新的介质或处理新的内容时，就有必要进行这些撤消表的读取处理，从而使处理复杂化。

并且，按照惯例，在把目标对准撤消未授权内容的处理的情况中，使用了存储未授权内容标识符的撤消表，和在把目标对准撤消未授权介质的处理的情况中，使用了存储未授权介质标识符的撤消表，并且，根据它们的用法，所涉及到的撤消是有差异的。在这种情况中，设备方需要从多个存储的撤消表中选择一个撤消表的处理，并且在这种选择之后进行与内容或介质标识符的核对。每当安装新的介质或处理新的内容时，就有必要重复进行这种撤消表选择处理，从而使处理复杂化。

发明内容

本发明提供了撤消对撤消表的这种未授权窜改和更新的结构，具体地说，本发明的目的是提供通过在撤消表中设置版本，在读出内容时将保存在设备中的撤消表的版本与内容标题中的有效撤消表的版本相比较，和在保存的表格的版本不是旧版本的条件下进行诸如内容的允许处理之类的处理，能够撤消由于未授权撤消表的滥用所导致的内容未授权使用的数据再现设备和数据记录设备、数据再现方法和数据记录方法、表格更新方法、和程序提供介质。

并且，本发明的另一个目的是提供通过在设备的存储器接口中设置版本，以便在设置之后，可以利用在存储器接口上的撤消表依次进行未授权介质和未授权内容的撤消，能够解决这种处理的复杂性问题，从而提高处理效率的数据再现设备和数据记录设备、数据再现方法和数据记录方法、表格更新方法、和程序提供介质。

并且，本发明的再一个目的是提供通过把属于不同类别的介质标识符和

内容标识符存储在单个撤消表中，从而无需选择撤消表的设备就能够把共享撤消表应用于介质和内容两者进行未授权介质和未授权内容的撤消，能够解决这种处理的复杂性问题，从而提高处理效率的数据再现设备和数据记录设备、数据再现方法和数据记录方法、表格更新方法、和程序提供介质。

根据本发明的第一方面，

对存储在数据存储装置中的内容执行再现处理的数据再现设备包括:

内部存储器，用于存储撤消表，撤消表是存储作为禁止处理对象的至少一个数据存储装置或内容的标识符的表格，该表格含有指示表格的新旧程度(newness)的版本信息；和

控制器，用于执行存储在作为再现对象的内容的标题信息中的有效撤消表版本与存储在内部存储器中的撤消表的版本之间的比较处理，和在确认存储在内部存储器中的撤消表的版本不旧（not older）于设置在作为再现对象的内容的标题信息中的版本的条件下，进行与作为再现对象的内容的再现同时进行的处理。

根据本发明的数据再现设备的实施例，控制器含有对存储在内部存储器中的撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符进行比较处理，作为与再现同时进行的处理的结构；和具有在存储在撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符在比较处理中相匹配的情况下，执行取消数据再现的处理的结构。

并且，根据本发明的数据再现设备的实施例，控制器含有执行对数据存储装置的存取的存储器接口、和执行对存储器接口的控制的控制单元；和存储器接口具有根据来自控制单元的数据再现请求命令，对存储在作为再现对象的内容的标题信息中的有效撤消表的版本与存储在内部存储器中的撤消表的版本进行比较处理的结构。

并且，根据本发明的数据再现设备的实施例，控制器含有对从外部接收的更新撤消表的版本与已经存储在内部存储器中的撤消表的版本进行比较处理，和在确认存储在内部存储器中撤消表的版本比更新撤消表的版本新的条件下，通过更新撤消表执行撤消表的更新处理的结构。

并且，根据本发明的数据再现设备的实施例，控制器具有根据数据完整

性检验值（ICV）执行与从外部接收的更新撤消表有关的数据窜改检验，和根据没有数据被窜改的判断通过更新撤消表执行撤消表的更新处理的结构。

根据本发明的第二方面，

对要存储在数据存储装置中的内容执行记录处理的数据记录设备包括：

内部存储器，用于存储撤消表，撤消表是存储作为禁止处理对象的至少一个数据存储装置或内容的标识符的表格，该表格含有指示表格的新旧程度的版本信息；和

控制器，用于执行把指定不参考撤消表进行再现处理的设置值设置成要存储在作为记录对象的内容的标题信息中的有效撤消表版本的处理，和对数据存储装置执行内容存储处理。

并且，根据本发明的数据记录设备的实施例，控制器含有执行对数据存储装置的存取的存储器接口、和执行对存储器接口的控制的控制单元；其中，存储器接口具有根据来自控制单元的伴随着数据记录的标题信息生成命令，执行把要存储在作为记录对象的内容的标题信息中的有效撤消表的版本设置成能够不参考撤消表进行再现的设置值的处理的结构。

并且，根据本发明的数据记录设备的实施例，控制器含有对从外部接收的更新撤消表的版本与已经存储在内部存储器中的撤消表的版本进行比较处理，和在确认存储在内部存储器中撤消表的版本比更新撤消表的版本新的条件下，通过更新撤消表执行撤消表的更新处理的结构。

并且，根据本发明的数据记录设备的实施例，控制器具有根据数据完整性检验值（ICV）执行与从外部接收的更新撤消表有关的数据窜改检验，和根据没有数据被窜改的判断通过更新撤消表执行撤消表的更新处理的结构。

根据本发明的第三方面，

用于对存储在数据存储装置中的数据执行再现处理的数据再现设备的数据再现方法包括：

比较步骤，对存储在作为再现对象的内容的标题信息中的有效撤消表版本与存储在数据再现设备的内部存储器中的撤消表的版本进行比较处理；和

再现相关处理执行步骤，在确认存储在内部存储器中的撤消表的版本不旧于设置在作为再现对象的内容的标题信息中的版本的条件下，进行与作为再现对象的内容的再现同时进行的处理。

并且，根据本发明的数据再现方法的实施例，再现相关处理执行步骤包

含对存储在内部存储器中的撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符进行比较处理的步骤；和在存储在撤消表中的至少一个数据存储装置或内容的标识符与作为再现对象的内容的标识符，或存储作为再现对象的内容的数据存储装置的标识符在比较处理中相匹配的情况下，执行取消数据再现的处理的步骤。

并且，根据本发明的数据再现方法的实施例，数据再现设备含有执行对数据存储装置的存取的存储器接口、和执行对存储器接口的控制的控制单元，数据再现方法还包括：把数据再现请求命令从控制单元发送到存储器接口的步骤；和根据数据再现请求命令在存储器接口上的接收，对存储在作为再现对象的内容的标题信息中的有效撤消表的版本与存储在内部存储器中的撤消表的版本进行比较处理的步骤。

并且，根据本发明的第四方面，

用于对要存储在数据存储装置中的内容执行记录处理的数据记录方法包括：

执行把指定不参考撤消表进行再现处理的设置值设置成要存储在作为记录对象的内容的标题信息中的有效撤消表版本的处理的步骤；和

对数据存储装置执行内容存储处理的步骤。

并且，根据本发明的第五方面，

用于数据处理设备的表格更新方法，把撤消表存储在内部存储器中，撤消表是存储作为禁止处理对象的至少一个数据存储装置或内容的标识符的表格，该表格含有指示表格的新旧程度的版本信息；其中，执行从外部接收的更新撤消表的版本与已经存储在内部存储器中的撤消表的版本之间的比较处理，和在确认存储在内部存储器中撤消表的版本比更新撤消表的版本新的条件下，通过更新撤消表执行撤消表的更新处理。

并且，根据本发明的表格更新方法的实施例还包括根据数据完整性检验值（ICV）执行与从外部接收的更新撤消表有关的数据窜改检验的步骤，其中，根据没有数据被窜改的判断，通过更新撤消表执行撤消表的更新处理。

并且，本发明的第六方面是

为对存储在数据存储装置中的数据执行再现处理的数据再现设备提供使数据再现处理可以在计算机系统上得以执行的计算机程序的程序提供介质，

其中，计算机程序包括:

比较步骤，对存储在作为再现对象的内容的标题信息中的有效撤消表版本与存储在数据再现设备的内部存储器中的撤消表的版本进行比较处理；和

再现相关处理执行步骤，在确认存储在内部存储器中的撤消表的版本不旧于设置在作为再现对象的内容的标题信息中的版本的条件下，进行与作为再现对象的内容的再现同时进行的处理。

并且，根据本发明的第七方面，

关于对存储在数据存储装置中的内容执行再现处理的数据再现设备;

数据再现设备具有把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中，和在存储器接口内的相继不同处理中，以可参考状态保存撤消表的结构。

并且，本发明的数据再现设备的实施例还包括对撤消表设置命令执行发送处理，作为在启动时的处理的控制单元，撤消表设置命令是与存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令；其中，存储器接口具有响应撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在存储器接口内进行参考处理的结构。

并且，根据本发明的数据再现设备的实施例，存储器接口具有根据数据完整性检验值（ICV）执行与读入存储器接口的撤消表有关的数据窜改检验，和在判断没有数据被窜改的条件下，执行能够在存储器接口内进行参考处理的撤消表设置处理的结构。

并且，根据本发明的数据再现设备的实施例，存储器接口具有从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

并且，根据本发明的数据再现设备的实施例，存储器接口具有从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

并且，根据本发明的数据再现设备的实施例，撤消表具有含有作为禁止处理对象的数据存储装置和作为禁止处理对象的内容两者的标识符数据的结

构。

并且，根据本发明的第八方面，

关于对要存储在数据存储装置中的内容执行记录处理的数据记录设备；

数据记录设备具有把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中，和在存储器接口的相继不同处理中，以可参考状态保存撤消表的结构。

并且，本发明的数据记录设备的实施例还包括对撤消表设置命令执行发送处理，作为在启动时的处理的控制单元，撤消表设置命令是与存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令；其中，存储器接口具有响应撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在存储器接口内进行参考处理的结构。

并且，根据本发明的数据记录设备的实施例，存储器接口具有根据数据完整性检验值（ICV）执行与读入存储器接口的撤消表有关的数据窜改检验，和在判断没有数据被窜改的条件下执行能够在存储器接口内进行参考处理的撤消表设置处理的结构。

并且，根据本发明的数据记录设备的实施例，存储器接口具有从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下取消数据记录处理的结构。

并且，根据本发明的数据记录设备的实施例，撤消表具有含有与作为禁止处理对象的数据存储装置和作为禁止处理对象的内容两者有关的标识符数据的结构。

并且，根据本发明的第九方面，

对存储在数据存储装置中的内容执行再现处理的数据再现方法包括：

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤；

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤；和

参考设置在存储器接口中的撤消表，判断数据再现处理是允许的还是不允许的步骤。

并且，本发明的数据再现方法的实施例还包括：对撤消表设置命令执行发送处理，作为在启动时的处理的步骤，撤消表设置命令是来自控制单元的、与对数据存储装置进行存取的存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令；和在存储器接口上，响应撤消表设置命令的接收，把撤消表读入存储器接口中，和执行撤消表设置处理，以便能够在存储器接口内进行参考处理的步骤。

并且，根据本发明的数据再现方法的实施例，根据数据完整性检验值（ICV）执行与读入存储器接口的撤消表有关的数据窜改检验，和在判断没有数据被窜改的条件下执行能够在存储器接口内进行参考处理的撤消表设置处理。

并且，本发明的数据再现方法的实施例还包括：在存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤。

并且，本发明的数据再现设备的实施例还包括：在存储器接口上，从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤。

并且，根据本发明的第十方面，

对要存储在数据存储装置中的内容执行记录处理的数据记录方法包括：

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤；

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤；和

参考设置在存储器接口中的撤消表，判断数据记录处理是允许的还是不允许的步骤。

并且，本发明的数据记录方法的实施例还包括：对撤消表设置命令执行发送处理，作为在启动时的处理的步骤，撤消表设置命令是来自控制单元的、与对数据存储装置进行存取的存储器接口有关的、用于保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表的设置命令；在存储器接口上，响应撤消表设置命令的接收，把撤消表读入存储器接口中，和

执行撤消表设置处理，以便能够在存储器接口内进行参考处理的步骤；和参考设置在存储器接口中的撤消表，判断数据记录处理是允许的还是不允许的步骤。

并且，根据本发明的数据记录方法的实施例，根据进行与读入存储器接口的撤消表有关的、基于数据完整性检验值（ICV）的数据窜改检验，和在判断没有数据被窜改的条件下，执行能够在存储器接口内进行参考处理的撤消表设置处理。

并且，本发明的数据记录方法的实施例还包括：在存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据记录处理的步骤。

并且，本发明的第十一方面是为了对存储在数据存储装置中的内容执行再现处理而提供使再现处理可以在计算机系统上得以执行的计算机程序的程序提供介质，其中，计算机程序包括：

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤；

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤；和

参考设置在存储器接口中的撤消表，判断数据再现处理是允许的还是不允许的步骤。

并且，本发明的第十二方面是为了对要存储在数据存储装置中的内容执行记录处理而提供使记录处理可以在计算机系统上得以执行的计算机程序的程序提供介质，其中，计算机程序包括：

把保存作为禁止处理对象的至少一个数据存储装置或内容的标识符数据的撤消表读入对数据存储装置进行存取的存储器接口中的步骤；

在存储器接口内的相继不同处理中，以可参考状态保存撤消表的步骤；和

参考设置在存储器接口中的撤消表，判断数据记录处理是允许的还是不允许的步骤。

根据本发明的第十三方面，

对存储在数据存储装置的内容执行再现处理的数据再现设备含有：

执行对数据存储装置的存取的存储器接口、和执行对存储器接口的控制的控制单元;

存储器接口含有

内部存储器，用于存储保存与作为禁止处理对象的数据存储装置和内容的每一个有关的标识符数据的撤消表;

其中，存储器接口含有从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构；和

其中，从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在设置在存储器接口中的撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

并且，根据本发明的数据再现设备的实施例，存储器接口根据来自控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据再现设备的实施例，存储器接口根据来自控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在相互验证处理期间接收数据存储装置标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据再现设备的实施例，存储器接口根据来自控制单元的数据再现请求命令，获取存储在要再现的内容的标题信息中的内容标识符，和在获取的内容标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据再现设备的实施例，存储器接口具有基于数据完整性检验值（ICV）执行与从外部接收的更新撤消表有关的数据窜改检验，从而判断没有数据被窜改的结构；和其中，执行从外部接收的更新撤消表的版本与已经存储在内部存储器中的撤消表的版本之间的比较处理，和在确认存储在内部存储器中的撤消表的版本比更新撤消表新的条件下，通过更新撤消表执行撤消表的更新处理。

并且，根据本发明的第十四方面，

对要存储在数据存储装置的内容执行记录处理的数据记录设备含有:

执行对数据存储装置的存取的存储器接口、和执行对存储器接口的控制的控制单元;

存储器接口含有内部存储器，用于存储保存与作为禁止处理对象的数据存储装置和内容的每一个有关的标识符数据的撤消表;

其中，存储器接口含有接收作为记录数据的对象的数据存储装置标识符，在接收的数据存储装置标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据记录处理的结构;

并且，根据本发明的数据记录设备的实施例，存储器接口根据来自控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据记录设备的实施例，存储器接口根据来自控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在相互验证处理期间接收数据存储装置标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的第十五方面，

关于对存储在数据存储装置的内容执行再现处理的数据再现方法;

在执行对数据存储装置的存取的存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理;

和从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的结构。

并且，本发明的数据再现方法的实施例还包括：在存储器接口上，根据来自控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据再现方法的实施例，在存储器接口上，根据来自控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在相互验证处理期间接收数据存储装置标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据再现方法的实施例，在存储器接口上，根据来

自控制单元的数据再现请求命令，获取存储在要再现的内容的标题信息中的内容标识符，和在获取的内容标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的第十六方面，

关于对要存储在数据存储装置的内容执行记录处理的数据记录方法；

在执行对数据存储装置的存取的存储器接口上，接收作为记录数据的对象的数据存储装置标识符，在接收的数据存储装置标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理；

并且，根据本发明的数据记录方法的实施例，在存储器接口上，根据来自控制单元的介质识别命令，接收作为介质的数据存储装置的标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，根据本发明的数据记录方法的实施例，在存储器接口上，根据来自控制单元的介质识别命令，与作为介质的数据存储装置进行相互验证处理，在相互验证处理期间接收数据存储装置标识符，和在接收的数据存储装置标识符与列在撤消表中的标识符之间执行核对处理。

并且，本发明的第十七方面是

为了对存储在数据存储装置中的内容执行再现处理而提供使再现处理可以在计算机系统上得以执行的计算机程序的程序提供介质，其中，计算机程序包括:

在执行对数据存储装置的存取的存储器接口上，从记录作为再现对象的数据的数据存储装置接收数据存储装置标识符，在接收的数据存储装置标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤；

和从存储在数据存储装置中的内容的标题信息中获取作为再现对象的内容的标识符，在获取的内容标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据再现处理的步骤。

并且，本发明的第十八方面是

为了对要存储在数据存储装置中的内容执行记录处理而提供使记录处理可以在计算机系统上得以执行的计算机程序的程序提供介质，其中，计算机程序包括:

在执行对数据存储装置的存取的存储器接口上，接收作为记录数据的对

象的数据存储装置标识符，在接收的数据存储装置标识符与列在撤消表中的标识符之间进行核对，和在标识符相互匹配的情况下，取消数据记录处理的步骤。

现在，与本发明相关的程序提供介质是以计算机可读格式把计算机程序提供给，例如，能够执行各种程序代码的通用计算机系统的介质。介质在形式上不特别限于，譬如，像 CD、FD、MO 那样的记录介质，或像网络那样的传输介质。

为了在计算机系统上实现特定计算机程序的功能，这样的程序提供介质定义了计算机程序与提供介质之间的结构性或功能性协同关系。换句话来说，通过提供介质把计算机程序安装在计算机系统中使协同关系在计算机系统上体现出来，因此，可以获得与本发明的其它方面相同的操作。

从基于本发明的下述实施例和附图的详细描述中，可以更清楚地看到本发明的其它目的、特征和优点。

附图说明

图 1 是说明使用根据本发明的数据处理设备的概念的图形；

图 2 是显示根据本发明的数据处理设备中的设备和介质的结构的图形；

图 3 是显示根据本发明的数据处理设备的存储器数据存储结构的图形；

图 4 是显示根据本发明的数据处理设备的设备的存储器接口的详细结构的图形；

图 5 是显示对于根据本发明的数据处理设备，在存储器接口的状态寄存器中的数据结构的图形；

图 6 是显示对于根据本发明的数据处理设备，存储在介质中的数据的详细结构的图形；

图 7 是说明对于根据本发明的数据处理设备，与存储在介质中的内容相对应地设置的保密标题的结构的图形；

图 8 是显示根据本发明的数据处理设备的数据加密的两种形式的图形；

图 9 是显示根据本发明的数据处理设备的撤消表的结构的图形；

图 10 是说明根据本发明的数据处理设备的块许可表（BPT（block permission table 的缩写）的图形；

图 11 是显示对于根据本发明的数据处理设备，在制造介质 1 时的 BPT

存储处理流程的图形；

图 12 是显示对于根据本发明的数据处理设备，在制造介质 2 时的 BPT 存储处理流程的图形；

图 13 是描述根据本发明的数据处理设备的块许可表（BPT）的具体例子的图形；

图 14 是说明根据本发明的数据处理设备的完整性检验值生成处理结构的图形；

图 15 是说明根据本发明的数据处理设备的完整性检验值生成处理流程的图形；

图 16 是说明对于根据本发明的数据处理设备，在启动设备时的流程的图形；

图 17 是说明根据本发明的数据处理设备的文件分配表的结构例子的图形；

图 18 是显示对于根据本发明的数据处理设备，在识别介质 1 时的流程（部分 1）的图形；

图 19 是显示对于根据本发明的数据处理设备，在识别介质 1 时的流程（部分 2）的图形；

图 20 是显示对于根据本发明的数据处理设备，在识别介质 2 时的流程（部分 1）的图形；

图 21 是显示对于根据本发明的数据处理设备，在识别介质 2 时的流程（部分 2）的图形；

图 22 是显示对于根据本发明的数据处理设备，在设备与介质之间执行的相互验证处理序列的图形；

图 23 是显示根据本发明的数据处理设备的相互验证／密钥共享处理流程（部分 1）的图形；

图 24 是显示根据本发明的数据处理设备的相互验证／密钥共享处理流程（部分 2）的图形；

图 25 是显示根据本发明的数据处理设备的文件读出处理流程的图形；

图 26 是显示根据本发明的数据处理设备的文件写入处理流程的图形；

图 27 是说明对于根据本发明的数据处理设备，存储在存储器中的数据的加密处理的形式的图形；

图 28 是说明能够作为对于根据本发明的数据处理设备，存储在存储器中的数据的加密处理的形式应用的三重 DES（数据加密标准）的图形；

图 29 是说明对于根据本发明的数据处理设备，存储在存储器中的数据的加密处理的形式的图形；

图 30 是说明对于根据本发明的数据处理设备，存储在存储器中的数据的加密处理的形式的图形；

图 31 是说明对于根据本发明的数据处理设备，完整性检验值以扇区为单位的存储处理的形式的图形；

图 32 是说明对于根据本发明的数据处理设备，与扇区相对应的内容密钥和其它密钥的加密处理的例子的图形；

图 33 是说明对于根据本发明的数据处理设备，与扇区相对应的内容密钥和其它密钥的解密处理的例子的图形；

图 34 是说明对于根据本发明的数据处理设备，在设备与介质之间，与扇区相对应的内容密钥和其它密钥的处理的例子的图形；

图 35 是显示对于根据本发明的数据处理设备，文件的解密读出处理流程（部分 1）的图形；

图 36 是显示对于根据本发明的数据处理设备，文件的解密读出处理流程（部分 2）的图形；

图 37 是显示对于根据本发明的数据处理设备，内容密钥和其它密钥的解密处理流程的图形；

图 38 是显示对于根据本发明的数据处理设备，通过介质存储密钥对内容密钥和其它密钥进行解密处理的流程的图形；

图 39 是显示对于根据本发明的数据处理设备，扇区数据的解密处理流程（部分 1）的图形；

图 40 是显示对于根据本发明的数据处理设备，扇区数据的解密处理流程（部分 2）的图形；

图 41 是显示对于根据本发明的数据处理设备，文件的加密写入处理流程（部分 1）的图形；

图 42 是显示对于根据本发明的数据处理设备，文件的加密写入处理流程（部分 2）的图形；

图 43 是显示对于根据本发明的数据处理设备，内容密钥和其它密钥的

加密处理流程的图形；

图 44 是显示对于根据本发明的数据处理设备，通过介质存储密钥对内容密钥和其它密钥进行加密处理的流程的图形；

图 45 是显示对于根据本发明的数据处理设备，扇区数据的加密处理流程（部分 1）的图形；

图 46 是显示对于根据本发明的数据处理设备，扇区数据的加密处理流程（部分 2）的图形；和

图 47 是显示根据本发明的数据处理设备的撤消表更新处理流程的图形。

具体实施方式

下面描述本发明的实施例。

[系统结构]

图 1 显示了可以把根据本发明的数据处理设备应用其中的内容分配系统结构。音乐数据、图像数据、和各种程序等之类的内容通过因特网之类的网络发送，或者，存储在各种记录介质，譬如，CD、DVD、或安装了闪速存储器的存储卡等之一的介质 103 上，并被设备 102 接收或被安装在设备 102 上，然后被执行。设备是具有内容再现功能的设备，例如，个人计算机（PC）、专用再现设备、游戏设备等，并且含有，例如，显示图像内容的显示设备、和用户输入指令的输入设备。

在这样内容分配系统的结构中，再现内容的设备和存储内容的介质的详细结构显示在图 2 中。

图 2 显示了设备 200、介质 210、和介质 230 的详细结构。介质 210 是含有只支持简单数据读出和写入处理的控制单元的介质，而介质 230 是含有控制器的介质，其中控制器与安装介质的设备进行相互验证处理，并且还对要存储在介质中的内容进行加密处理。介质 210 和介质 230 都可以安装到设备 200 上。

图 2 所示的设备 200 含有通信单元 201，用于通过因特网之类的数据通信手段进行数据发送／接收处理；输入单元 202，用于输入各种指令；显示单元 203，用于进行消息和内容等的显示；设备控制器 204，含有对这些单元进行控制的控制单元 205 和对于数据输入／输出处理，具有与介质的交接

功能的存储器接口（I／F）单元 300；和存储单元 207，用作存储未授权介质的内容文件组和撤消表和作为失效信息的内容。请注意，诸如撤消表等之类存储在内部存储器中的数据文件具有能够通过文件分配表进行管理和被读出的结构。

在再现内容时，一旦确认作为再现对象的内容不与存储在撤消表中的无效介质或无效内容相对应，设备 200 就进行再现。在作为再现对象的内容列在撤消表中的情况下，出现再现错误，因此，不执行再现处理。以后再详细描述撤消表和应用撤消表的再现处理。

介质 1，即介质 210 含有控制单元 211，用于控制数据输入／输出；存储单元 212，用于存储内容，其中，存储单元 212 不仅存储与相应标题信息一起的内容，而且存储对于每个介质来说是唯一标识信息的介质 ID，此外，还存储作为描述存储器存取控制信息的存取许可表的 BPT（块许可表）。

在识别了介质之后，设备 200 的文件系统从介质读取作为存取许可表的 BPT，把 BPT 传输到在那里得到管理的、对介质进行直接存取的存储器接口单元 300。一旦接收到 BPT，存储器接口单元 300 就对与接收的 BPT 有关的完整性检验值（ICV）进行确认。只有在 ICV 被判断为得到验证的情况下，才把 BPT 存储成有效的。在接收存取介质的存储器的命令的情况下，存储器接口单元 300 只执行基于介质的 BPT 的存取。以后再详细描述 BPT 的结构和利用 BPT 的处理。

介质 2，即介质 230 由控制器 231 和存储单元 232 构成，其中，存储单元 232 存储与相应标题信息一起的内容，并且还存储作为存取许可表的 BPT（块许可表）。控制器 231 含有存储器接口（I／F）单元 234，用作存储单元 232 的数据存储或数据读出接口；和介质 2 ID，用作介质的标识符；内部存储器 235，用于存储应用于相互验证处理的验证密钥 Kake、作为把内容存储到存储单元 232 时使用的加密密钥的存储密钥 Ksto、以及在加密作为加密对象的密钥时的初始值 IV_keys 等；加密处理单元 236，含有寄存器，用于执行内容的验证处理或加密／解密处理；和控制单元 233，用于控制这些部件。

[介质中的存储结构]

接着，介质 210 和介质 230 的存储单元的数据存储结构显示在图 3 中。存储单元是，例如，闪速存储器，闪速存储器是一种被称为 EEPROM（电可

擦除可编程只读存储器）的、可电重写的非易失性存储器，和数据擦除是按块递增方式，通过分批擦除进行的。

如图 3（a）所示，闪速存储器含有多个块，即第 1 块到第 N 块，如图 3（b）所示，每个块由多个扇区，即第 1 扇区到第 M 扇区构成，和如图 3（c）所示，每个扇区由包含实际数据的数据部分、和包含纠错码等之类的冗余数据的冗余部分构成。尽管后面会作详细描述，但是这里说明一下，每个扇区的数据部分内用作扇区数据完整性检验值的 ICV 可以存储在冗余部分中。

[基本命令]

接着，描述在图 2 所示的设备 200 中，在控制单元 205 和存储器接口（I／F）单元 300 上发出的基本命令。

首先，从控制单元 205 到存储器接口（I／F）单元 300 的命令包括如下:

•状态读出命令

读取存储器接口中被设置成当前状态的状态寄存器的状态。存储器接口（I／F）单元 300 返回状态寄存器的内容。

•扇区读出命令

特定扇区的数据读出处理命令。

•扇区写入命令

对特定扇区的数据写入处理命令。

•扇区解密读出命令

根据设置标题中的信息，执行解密特定扇区的加密数据和读出它的处理的命令。

•扇区加密写入命令

根据设置标题中的信息，执行加密数据和将它写入特定扇区的处理的命令。

•标题生成命令

根据特定参数，执行生成标题的处理的命令。

•标题设置命令

执行在存储器接口内设置标题的处理的命令。

•BPT 设置命令

执行在存储器接口内设置 BPT 的处理的命令。

•撤消表设置命令

执行在存储器接口内设置作为未授权介质和未授权内容的表格的撤消表的处理的命令。

•更新撤消表检验命令

执行检验撤消表是否是可接受的，以便把当前撤消表更新成更新撤消表的处理的命令。

•介质 1 识别命令

执行读出介质 1 的介质标识符（ID），和检验 ID 是否有效的处理的命令。

•介质 2 识别命令

执行与相连的介质 2 进行相互验证，和检验介质标识符（ID）是否有效的处理的命令。

•文件分配表取出命令

执行读取存储器内的文件分配表的处理的命令。

•文件分配表更新命令

执行对存储器更新文件分配表的处理的命令。

从存储器接口（I／F）单元 300 到介质 1 的命令包括如下命令。

•ID 读出命令

执行读出介质 1 拥有的 ID 的处理的命令。

[设备内存储器接口的详细结构]

接着，设备 200 内存储器接口（I／F）单元 300 的详细结构显示在图 4 中。现在描述它的各个部件的功能。

•状态寄存器 301

用于存储存储器接口的内部状态的寄存器。状态寄存器的结构例子显示在图 5 中。每一位具有如下含义。

•位 0：忙标志（1：忙，0：就绪）

用于判断存储器接口是否正在进行内部处理的位。

•位 1：读出成功标志（1：成功，0：失败）

用于判断数据从存储器的读出是否取得成功的位。

•位 2：写入成功标志（1：成功，0：失败）

用于判断数据到存储器的写入是否取得成功的位。

•位 3：介质 1 设置标志（1：设置，0：未设置）

用于判断相连介质 1 是否可用的位。

•位 4：介质 2 设置标志（1：设置，0：未设置）

用于判断相连介质 2 是否可用的位。

•位 5：介质 1 有效标志（1：有效（OK），0:无效（不好））

用于判断相连介质 1 的标识符（ID）是否是撤消表内要被撤消的介质对象的位。

•位 6：介质 2 有效标志（1：有效（OK），0:无效（不好））

用于判断相连介质 2 的标识符（ID）是否是撤消表内要被撤消的介质对象的位。

•位 7：标题设置成功标志（1：成功，0：失败）

用于判断标题是否在存储器接口内已经被成功设置的位。

•位 8：标题生成成功标志（1：成功，0：失败）

用于判断标题的生成是否已经取得成功的位。

•位 9：撤消表设置标志（1：设置，0：未设置）

用于判断撤消表是否在存储器接口内已经被成功设置的位。

•位 10：更新撤消表有效标志（1：有效（OK），0:无效（不好））

用于判断更新撤消表是否有效的位。

状态寄存器 301 拥有这些存储器接口（I／F）单元 300 的状态信息。

返回到图 4，让我们继续描述各个部件的功能。

•命令寄存器 302

用于存储从控制单元发送的命令的寄存器。

•地址寄存器 303

用于设置数据传输开始扇区的寄存器。

•计数寄存器 304

用于设置要传输的数据的总扇区数的寄存器。

请注意，从外部存储器和内部存储器读出数据和把数据写入外部存储器和内部存储器是通过在地址寄存器中设置开始读出或写入的扇区地址，在计数寄存器中设置要读出或写入的总扇区数，和在命令寄存器中设置扇区读出／写入命令来执行的。

•控制寄存器 305

用于设置存储器接口的动作的寄存器。

•发送／接收控制单元 306

对存储器接口，譬如，各种寄存器和发送／接收缓冲器进行控制。

•发送缓冲存储器 307

用于存储发送数据的缓冲器。

•接收缓冲存储器 308

用于存储接收数据的缓冲器。

•发送寄存器 309

用于发送发送缓冲存储器 307 内的数据的寄存器。

•接收寄存器 310

用于存储接收数据和把它传输到缓冲存储器 308 的寄存器。

•加密处理单元 320

对发送缓冲存储器 307 和接收缓冲存储器 308 内的数据进行各种加密处理。

•存储单元 321

用于存储和保存加密处理单元 320 进行加密处理所需的密钥信息、从内部存储器中读取的撤消表、和从内部存储器中读取的用作存取许可表的块许可表（BPT）的区域。在撤消表和块许可表（BPT）在存储器接口内被设置成有效的情况下，和在发送／接收控制单元 306 从控制单元接收介质识别命令或在内部存储器中读／写有关数据的命令的情况下，如此等等，参照设置的撤消表和块许可表（BPT）进行处理。这样的处理以后参照流程图再作详细描述。

并且，把如下数据存储在存储单元 321 中，作为加密处理所需的密钥信息。

Kdist: 包含在除了存储在介质 2 中的内容之外的内容的保密标题中的分配密钥。加密生成密钥 Kicv_cont 和内容密钥 Kc 的内容。

Kicv_sh: 在生成保密标题的 ICV 时使用的保密标题 ICV 生成密钥。

Ivsh: 用于生成保密标题的 ICV 的初始值（IV: 初始值）。

Mkake: 用于相互验证的主密钥。

Ivake: 应用于用于相互验证的密钥的生成处理的初始值（IV: 初始值）。

Ivauth: 用于生成用于相互验证的数据的初始值（IV: 初始值）。

Mkicvr_rl: 用于生成用于撤消表的 ICV 密钥的主密钥。

Ivicv_rl: 当生成用于撤消表的 ICV 密钥时使用的初始值（IV: 初始值）。

Ivr1: 当生成用于撤消表的 ICV 时使用的初始值（IV: 初始值）。

IV_keys: 当在介质 2 上加密内容加密密钥时使用的初始值（IV: 初始值）。

Mkicv_bpt: 用于生成用于作为存取许可信息的 BPT（块许可表）的 ICV 密钥的主密钥。

IVicv_bpt: 当生成用于作为存取许可信息的 BPT（块许可表）的 ICV 密钥时使用的初始值（IV: 初始值）。

IVbpt: 用于作为存取许可信息的 BPT（块许可表）的初始值（IV: 初始值）。

•ECC 电路 323

对发送寄存器 309 和接收寄存器 310 中的数据进行 ECC 检验的专用模块。

•外部存储器输入／输出接口 324

用于外部存储器（介质 1 和 2）的输入／输出接口。外部存储器的例子有安装闪速存储器的存储卡等。例如，内容、与内容的记录／再现同时出现的标题信息、以及块许可表（BPT）都通过这个外部存储器输入／输出接口输入和输出。

•内部存储器输入／输出接口 325

用于内部存储器的输入／输出接口。通过这个接口对，例如，存储在内部存储器中的撤消表进行输入和输出。

与处理相对应，如下的信号从外部存储器输入／输出接口 324 和内部存储器输入／输出接口 325 输出到外部存储器（介质 1 和 2）或内部存储器。

CLE: 命令锁存使能

ALE: 地址锁存使能

CE: 芯片使能

WE: 写使能

RE: 读使能

此外，作为来自外部存储器（介质 1 和 2）或来自内部存储器的信号，

WP: 写保护（只应用于外部存储器（介质 1 和 2）

RDY／BUSY: 就绪／忙

这些信号是输入信号。

[存储在存储器中的内容的结构]

接着，参照图 6 描述存储在介质的闪速存储器中的内容的结构。如图 6（a）所示，像音乐数据和图像数据等那样的内容包括由各种属性信息构成的保密标题和作为实际数据部分的内容。

如图 6（b）所示，多个内容的保密标题部分和内容部分成对存储在介质的闪速存储器中。如上所述，闪速存储器以块为单元被擦除，因此，一个块存储与同一内容相关的标题部分、或内容部分，并且，除了允许成批擦除处理的情况外，不进行把不同内容存储在一个块中的处理。

[保密标题的结构]

保密标题是与内容有关的属性信息。保密标题的数据结构显示在图 7 中。下面描述每段数据的内容。

•格式版本

指示保密标题的格式版本。

•内容 ID

指示内容的标识符（ID）。

•内容类型

指示内容的类型。例如，存储在介质 1 和 2 中的内容、或广播内容等。

•数据类型

指示内容的属性，例如，是像音乐、图像等那样的数据，还是程序，等。

•加密算法

指示利用内容密钥（Kc）的加密处理算法。例如，指示加密是否是通过 DES、Triple-DES 等进行的。

•加密模式

指示与加密算法规定的算法有关的加密模式。例如，指示是 ECB 模式，还是 CBC 模式等。

•加密格式类型

指示内容的加密格式。

用一个内容密钥 Kc 加密整个内容的类型是类型 1，和通过应用于内容的每个扇区的不同密钥 Ksec_n 加密内容的类型是类型 2。

图 8 显示了每种类型的加密格式结构。图 8（a）显示了通过类型 1 加密格式加密的内容的存储器存储结构，和图 8（b）显示了通过类型 2 加密

格式加密的内容的存储器存储结构。

图 8（a）所示的类型 1 加密格式是所有内容用一个密钥 Kc 加密和存储在存储器中的结构，即，扇区无关加密处理。图 8（b）所示的类型 2 加密格式是把不同扇区密钥 Ksec_1 到 Ksec_m 应用于闪速存储器的每个扇区和存储加密内容的结构，即，扇区相关加密处理。例如，对于图 8（b）中闪速存储器的扇区 1，把 Ksec_1 设置成与扇区 1 相对应的加密密钥，和要存储在扇区 1 中的内容都经历应用 Ksec_1 的加密处理，并且存储在每个块中。对于闪速存储器的扇区 m，把 Ksec_m 设置成与扇区 m 相对应的加密密钥，和要存储在扇区 m 中的内容都经历应用 Ksec_m 的加密处理，并且得到存储。

这样，对于本发明的结构，应用把不同加密密钥应用于每个扇区的内容加密处理。并且，可以把各种加密形式应用于把不同加密密钥应用于每个扇区的处理形式，譬如，把一个密钥应用于一个扇区的单重 DES 处理，通过把多个密钥应用于一个扇区的三重 DES 的处理，等等。以后再详细描述这些处理形式。

现在，让我们回到图 7，继续描述保密标题的结构。

•加密标志

指示一个块内每个扇区的加密／未加密的标志。标志数与一个块中的扇区数（例如，32 个扇区）一样多。例如，0：非加密扇区，1：加密扇区。在本实施例中，一个块有 32 个扇区。

•ICV 标志

指示一个块内每个扇区的 ICV 附加／不附加的标志。标志数与一个块中的扇区数（例如，32 个扇区）一样多。例如，0：没有 ICV，1：附加了 ICV。

•加密内容密钥（Kc_Encrypted 0-31）

用于加密内容密钥（32 个）的存储区。

•加密 ICV 生成密钥（Kicv_cont_encrypted）

用于创建与加密内容有关的 ICV 的密钥的存储区。

•有效撤消表版本

可有效应用于内容再现的撤消表的版本。

在所设置的撤消表的版本比再现内容时撤消表的版本旧的情况下，不允许再现。此外，对于不需要参考撤消表的内容，设置成 0，譬如，存储的数据的再现处理在自己的设备内进行等。

•加密标题的 ICV

加密标题的完整性检验值（ICV）

[撤消表]

接着，描述作为未授权介质和内容的失效信息的撤消表的结构。图 9 显示了撤消表的结构。下面描述每种类型的数据。

•撤消表 ID

用作对于撤消表来说是唯一的标识符的 ID。

•撤消表版本

指示撤消表的版本。更新撤消表，和在更新时加入新的未授权介质和内容的失效信息。

对于本发明的结构，把版本信息设置在撤消表中，和把有效撤消表的版本信息设置在内容的标题中。在读出内容时，将设备当前保存的撤消表的版本与内容的标题中的撤消表的版本加密比较。同时，在当前保存的撤消表的版本是较旧的情况下，取消内容的读出。因此，如果不更新撤消表，就不能读出内容。

此外，在更新撤消表时，存储器接口将当前撤消表的版本信息与更新撤消表的版本信息相比较，和只有在判断撤消表是新的情况下，才允许更新撤消表。

以后参照处理流程图再详细描述撤消表利用版本信息的新／旧比较处理，以及更新处理的具体处理的例子。

•介质 1 ID 的个数

无效介质 1（介质 1 ID）的总个数。

•介质 1 ID（0）到介质 1 ID（L-1）

无效介质 1 的一系列标识符。

•介质 2 ID 的个数

无效介质 2（介质 2 ID）的总个数。

•介质 2 ID（0）到介质 2 ID（M-1）

无效介质 2 的一系列标识符。

•内容 ID 的个数

无效内容 ID 的总个数

•内容 ID（0）到内容 ID（N-1）

一系列无效内容标识符。

•撤消表的 ICV

用于对撤消表进行窜改检验的 ICV。

如上所述，根据本发明的撤消表由多种类型（介质，内容）的标识符构成。这样，通过在作为内容和介质的失效信息的撤消表中，提供作为撤消对象的多种类型的 ID，即，介质 ID 和内容 ID，并且可以作为不同的操作进行它们的核对处理，可以用单个撤消表撤消多个内容和介质。在插入介质或读出内容时，通过在所使用的介质或所使用的内容的标识符（ID）与列在存储器接口单元上的撤消表中的 ID 之间进行核对，可以禁止未授权介质的使用和未授权内容的读出。

这样，由于把多个内容和介质的 ID 设置在单个撤消表中的结构，可以用单个撤消表撤消多种类型的介质和内容。以后将描述在启用介质时介质基于撤消表的确认处理，和在处理内容时内容确认处理的具体处理。

此外，对于本发明的结构，把撤消表设置到直接存取外部存储器等的存储器接口中，并且，在设置之后，当安装介质时或当再现内容时，可以在存储器接口上不断使用撤消表，这样就避免了诸如在使用内容时，从内部存储器重复读出之类的处理，从而，可以有效地进行处理。

[块许可表（PBT）]

接着，描述用作存取许可表的块许可表（BPT）的结构。按照惯例，在，例如，在个人计算机等上进行内容的再现的情况下，个人计算机的操作系统的文件系统主观地读出和管理存储在记录介质中的存取信息表（例如，文件分配表（FAT）），和文件系统已经能够自由地重写存取信息表的内容。因此，即使在存在存储设置成禁止写入的存取信息表的记录介质的情况下，也存在着记录介质内的数据可能被读取那个存取信息表和重写它的文件系统重写的可能性。

根据本发明的数据处理设备所应用的块许可表（BPT）是存储在禁止被设备重写的块的、介质本身的存取许可表。在设备利用存储 BPT 的介质，执行诸如重写内容数据等之类的数据处理的情况下，把块许可表（BPT）设置在直接存取介质的设备的存储器接口单元中，从而，与设备的控制单元执行哪个程序无关，在许可信息被设置在作为介质的存取许可表的块许可表（BPT）中之后，进行存储器存取。

图 10 显示了块许可表（BPT）的结构。现在描述每组数据。

•格式版本

指示 BPT（块许可表）的格式版本。对于 PBT 本身，也存在着各种格式，这是标识是其中的哪一个的数据。

•BPT 标识符（BPT ID）

块许可表（BPT: 块许可表）的标识符（ID）。

•块数（块的个数）

指示 BPT（块许可表）管理的总块数。如上所述，闪速存储器是按块递增方式擦除的。这指示 BPT 管理的块数。

•块 # 1 到块 # n 许可标志

指示每个块的存取限制标志。例如，这指示，标志 0 的块是不可擦除块，和标志 1 的块是可擦除块。

•BPT-ICV（BPT 的 ICV）

用于对 BPT（块许可表）进行窜改检验的 ICV。

在识别出设备之后，设备的文件系统接着从诸如存储卡等之类安装了闪速存储器的介质中读出块许可表（BPT），把 BPT 传输到直接存取介质的存储器接口，和让 BPT 作为存取许可表对那个介质进行管理。存储器接口单元接收存取许可表，并且设置 BPT（例如，图 4 所示的存储单元 321）。一旦接收到存取介质的存储器的命令，存储器接口只执行基于这个介质的存取许可表的存取。

在块许可表（BPT）中进行设置，譬如，按照介质的闪速存储器的块的递增方式许可的处理形式，具体地说，与，例如，可擦除块、不可擦除块、可再现块、不可再现块等有关的设置。在 BPT 设置之后，存储器接口确定处理是否是许可的。以后将更详细地描述这样的处理的细节。

此外，为了防止窜改，把完整性检验值 ICV 设置在块许可表（BPT）中，并且，在把 BPT 设置到存储器接口中时，进行 ICV 检验，和在判断已经被窜改了的情况下，不进行 BPT 设置处理。因此，可以防止创建和使用未授权存取许可表。BPT 的 ICV 是根据介质标识符（ID）生成的。因此，即使在存取许可表被复制到另一个介质中的情况下，也不能使用那个介质。以后将描述 ICV 的生成。

块许可表（BPT）是在制造存储器（例如，闪速存储器）时，被写入存

储器的预定块中的，然后被运走。现在，描述在用于存储了块许可表（BPT）的存储器内的块的块许可表（BPT）中的块不可擦除设置。对于根据本发明的设备，在擦除存储在介质中的数据的处理过程中，参考 BPT，和参考如在 BPT 中所设置的那样，每个块的擦除是否是许可的，在此之后，只擦除可擦除块，从而，对于 BPT 存储块被设置成不可擦除的介质，防止了 BPT 被擦除和重写。以后将描述利用介质内的 BPT 对文件进行写入和再现处理。

图 11 和图 12 显示了在制造介质（安装了闪速存储器的数据记录介质）时，设置块许可表（BPT）的流程。这里，让我们假设，通过可以与介质进行命令通信的介质创建设备生成介质标识符（ID）和写入 BPT 是连续操作。

图 11 是对于不具有相互验证处理功能的介质 1 的类型，介质创建设备执行的、块许可表（BPT）的设置流程图。现在描述每个处理。首先，把 ID 读出命令发送到还没有进行初始化设置的介质（S31），和一旦接收到事先存储在介质中的 ID（S32），就根据 ID 生成 ICV 生成密钥 Kicv_bpt（S33）。根据主密钥 MKicv_bpt、初始值 IVicv_bpt、和 BPT 标识符（ID）生成 ICV 生成密钥 Kicv_bpt。具体地说，这是根据 ICV 生成密钥 Kicv_bpt = DES（E，MKicv_bpt，ID^IVicv_bpt）生成的。这个方程的含义是根据 BPT 的 ID 和初始值 IVicv_bpt 的异或运算结果，利用主密钥 MKicv_bpt，在 DES 模式下进行加密处理。

接着，把必要的参数设置在 BPT 的各个栏目中（S34），和根据设置了参数的 BPT（应用如后面参照图 14 所述的结构）生成 ICV（S35），把生成的 ICV 设置在 BPT 的 ICV 栏目中（S36）。把如此构成的块许可表（BPT）写入介质 1 中（S37）。如上所述，写入 BPT 的块成为在 BPT 中被设置成不可擦除区的块。

图 12 是对于具有相互验证处理功能的介质 2 的类型，介质创建设备执行的设置块许可表（BPT）的流程图。现在描述每个处理。首先，与还没有进行初始化设置的介质 2 进行相互验证处理和会话密钥共享处理（对于这些处理过程，请参见如图 22 所示的处理）（S41）。

相互验证处理和密钥共享处理一结束，就把 ID 读出命令发送到介质 2（S41），然后，读出 ID，并且根据 ID 生成 ICV 生成密钥 Kicv_bpt（S42）。根据主密钥 MKicv_bpt、初始值 IVicv_bpt、和 BPT 标识符（ID）生成 ICV 生成密钥 Kicv_bpt。具体地说，这是根据 ICV 生成密钥 Kicv_bpt = DES（E，

MKicv-bpt，ID^IVicv-bpt）生成的。这个方程的含义是根据 BPT 的 ID 和初始值 IVicv-bpt 的异或运算结果，利用主密钥 MKicv-bpt，在 DES 模式下进行加密处理。

接着，把必要的参数设置在 BPT 的各个栏目中（S43），和根据设置了参数的 BPT（应用如后面参照图 14 所述的结构）生成 ICV（S44），把生成的 ICV 设置在 BPT 的 ICV 栏目中（S45）。把如此构成的块许可表（BPT）写入介质 2 中（S46）。如上所述，写入 BPT 的块成为在 BPT 中被设置成不可擦除区的块。

图 13 显示了块许可表（BPT）的具体结构例子。图 13（a）是介质 1 和介质 2 的闪速存储器的块结构，和图 13（b）是块许可表（BPT）。块许可表（BPT）具有如下结构，在格式版本、BPT ID 和块数之后，设置每个块是可擦除的（1），还是不可擦除的（0），最后，存储 BPT 的完整性检验值（BPT 的 ICV）。存储器的 BPT 存储块（在图 13 的例子中，块＃2）在块许可表（BPT）中被设置成不可擦除区，从而，提供了防止设备擦除的结构，并且不进行 BPT 的重写。

现在，图 13 所示的块许可表（BPT）的结构例子是只设置了每个块是可擦除的（1），还是不可擦除的（0）的结构，但是，还可以作出允许，还是不允许读出（再现）的安排，来代替对于擦除处理，只设置存取许可的结构。例如，可以作出这样的设置，不允许再现和擦除（11）、可再现或不可擦除（10）、不可再现但可擦除（01）、和可再现和可擦除（00）。

现在，如图 2 所示，介质 2 拥有在介质内的控制单元 231，使得可以存储是否设置块许可表（BPT）的状态，因此，可以使用防止 BPT 被重写的结构，对于在设置了 BPT 的状态下，从设备传来新的 BPT 写入命令的结构，这些命令是不被接受的。

应该注意到，在上面例子中的 BPT 写入已经参照通过可以与介质进行命令通信的介质创建设备执行的结构作了描述，但是，取而代之，结构也可以是这样的，BPT 到介质的写入通过直接写入的简单存储器写入程序创建的 BPT 来进行。但是，在这种情况中，存储器的 BPT 存储块在块许可表（BPT）中也被设置成不可擦除区。

[通过完整性检验值（ICV）的窜改检验]

接着，描述利用完整性检验值（ICV：完整性检验值）的窜改检验处理。

在本发明的结构中，把完整性检验值（ICV）加入存储在数据存储装置中的内容、块许可表、撤消表等中，并且对内容、块许可表、撤消表等的每一个应用数据窜改检验处理。与内容有关的完整性检验值具有可以按扇区数据递增的方式加入的结构。以后将描述加入内容、块许可表、撤消表等中的、ICV处理的特定形式。

利用 DES 加密处理结构生成完整性检验值（ICV）的例子显示在图 14 中。如图 14 的结构所示，构成作为对象的窜改检验数据的消息被划分成 8-字节单元（被分割的消息后面称之为 D0、D1、D2、……Dn-1）。窜改检验数据可以是，例如，内容本身，可以是作为上述存取许可表的 BPT 的配置数据、或者，可以是撤消表的配置数据。

首先，对初始值（下面称为 IV）和 D0 进行异或运算（把它的结果取为 I1）。接着，把 I1 放入 DES 加密单元中，利用完整性检验值（ICV）进行加密，生成密钥 Kicv（把它的输出取为 E1）。接着，对 EQ 和 D1 进行异或运算，把它的输出 I2 放入 DES 加密单元中，利用完整性检验值（ICV）进行加密，生成密钥 Kicv（输出 E2）。随后，重复这些处理，和对消息的所有部分进行加密处理。把最后输出的 EN 取为内容完整性检验值 ICV′。

在证明了保证没有被窜改的授权 ICV，例如，在生成内容时生成的一个，与根据内容新生成的 ICV′相同的情况下，即，在 ICV′＝ICV 的情况下，保证了诸如内容、BPT 或撤消表等之类的输入消息未被窜改，但是，在 ICV′≠ICV 成立的情况下，判断已经被窜改了。

图 15 显示了利用 ICV 的数据窜改检验处理流程。首先，提取作为窜改检验对象的数据（S11），和根据提取的数据，通过，例如，图 14 所示的 DES 加密处理结构计算 ICV′（S12）。作为计算的结果，将计算的 ICV′与存储在数据中的 ICV 相比较（S13），并且，在它们相匹配的情况下，判断数据未被窜改，因此，数据是有效的（S14 到 S15），和在它们不相匹配的情况下，判断数据被窜改（S14 到 S16）。

根据用于生成事先存储在设备的存储器接口单元 300 的存储单元 321（参见图 4）中的撤消表的 ICV 密钥的主密钥 MKicv_r1、供生成撤消表的 ICV 密钥时使用的初始值 IVicv_r1、和包含在撤消表的属性信息中的撤消表版本，生成用于撤消表窜改检验的完整性检验值（ICV）生成密钥 Kicv_r1。具体地说，这是根据完整性检验值（ICV）生成密钥 Kicv_r1＝DES（E，MKicv_r1，

Version^IVicv-r1）生成的。这个方程的含义是根据版本与初始值（IVicv-r1）的异或运算结果，利用主密钥 MKicv-r1，在 DES 模式下进行加密处理。撤消表的完整性检验值检验是由图 15 所示的 ICV 生成结构应用如此生成的完整性检验值（ICV）生成密钥 Kicv-r1 和利用这个初始值 IVicv-r1（存储在存储单元 321 中）来执行的。

此外，根据用于生成事先存储在设备存储器接口单元 300 的存储单元 321（参见图 4）中的 BPT 的 ICV 密钥的主密钥 MKicv-bpt、供生成 BPT 的 ICV 密钥时使用的初始值 IVicv-bpt、和包含在 BPT 属性信息中的 BPT 标识符，生成用于块许可表(BPT)窜改检验的完整性检验值(ICV)生成密钥 Kicv-bpt。具体地说，这是根据完整性检验值（ICV）生成密钥 Kicv-bpt = DES（E，MKicv-bpt，ID^IVicv-bpt）生成的。这个方程的含义是根据 BPT ID 与初始值（IVicv-bpt）的异或运算结果，利用主密钥 MKicv-bpt，在 DES 模式下进行加密处理。块许可表（BPT）的完整性检验值检验是由图 15 所示的 ICV 生成结构应用如此生成的完整性检验值（ICV）生成密钥 Kicv-bpt 和利用这个初始值 IVicv-bpt（存储在存储单元 321 中）来执行的。并且，作为 BPT 的辅助信息存储的 ICV 是根据 BPT 内的数据和包含存储 BPT 的介质的标识符（ID）的数据生成的。因此，BPT 的 ICV 检验不仅起核实 BPT 的数据是否被窜改的作用，而且起核实 BPT 对于介质来说是否是唯一有效的，即，是否不是被复制到其它独立介质的 BPT 的作用。

此外，加密用于按扇区递增的方式进行内容的窜改检验的完整性检验值（ICV）生成密钥 Kicv-cont，将其存储在内容的标题（保密标题）中，和在需要的时候，由存储器接口的加密处理单元 320（参见图 4），或通过与介质 2 进行相互验证之后执行的、由介质 2 的控制器 231 执行的、利用 DES-CBC 模式的解密处理获得它。在利用流程图的描述中将详细描述这些处理。

在这样的数据窜改检验得出，例如，显而易见，撤消表被窜改了的情况下，禁止根据参考撤消表的处理再现内容等，和在判断作为存取许可表的 BPT 表被窜改了的情况下，执行处理，以便禁止根据 BPT 存取介质的数据。以后将详细描述这些处理。

[数据读出、写入处理]

下面描述利用根据本发明的数据处理设备，在设备从介质中读出数据的情况下和在设备把数据写入介质中的情况下的处理。

（在启动设备时的处理）

首先，参照图 16 描述在启动设备的情况下的处理。在图 16 中，左边显示了设备 200 的控制单元 205 的处理，右边显示了存储器接口单元 300 的处理。在开始处理那一时刻，存储器接口单元 300 的状态寄存器是：忙标志：0（就绪），撤消表设置标志：0（未设置）。

首先，一旦设备被启动，控制单元就把内部存储器中文件分配表取出命令发送到存储器接口单元（S101）。存储器接口单元把文件分配表读出命令发送到设备的内部存储器（S102），从内部存储器接收文件分配表，和把它发送给控制单元（S103）。

现在，文件分配表是对可由设备和外部存储器存取的、存储在内部存储器中的数据，例如，各种内容、撤消表等的各种数据文件进行目录管理，和如图 17 所示，具有将目录、文件名、和存储扇区相互联系在一起的结构的表格。设备根据文件分配表存取各种文件。

一旦接收到存储在内部存储器中的与数据相对应的文件分配表（S104），控制单元就根据该表格执行撤消表的读出处理（S105），并且把撤消表设置命令和撤消表发送到存储器接口（S106）。撤消表的设置处理只在撤消表有效的情况下执行，并且，一旦对该表格进行了设置，就在处理内容，例如，从介质中读出内容等时，利用列在撤消表中的内容或介质标识符进行比较处理。以后将描述这些处理。

一旦从控制单元接收到撤消表设置命令和撤消表（S107），存储器接口就把状态寄存器的忙标志设置成 1（忙）（S108），并且生成用于撤消表窜改检验的完整性检验值（ICV）生成密钥 Kicv_r1（S109）。

用于撤消表窜改检验的完整性检验值（ICV）生成密钥 Kicv_r1 是根据用于生成事先存储在设备内的撤消表的 ICV 密钥的主密钥 MKicv_r1、供生成撤消表的 ICV 密钥时使用的初始值 IVicv_r1、和包含在撤消表的属性信息中的撤消表版本生成的。具体地说，这是根据完整性检验值（ICV）生成密钥 Kicv_r1 = DES（E，MKicv_r1，Version^IVicv_r1）生成的。这个方程的含义是根据版本与初始值（IVicv_r1）的异或运算结果，利用主密钥 MKicv_r1，在 DES 模式下进行加密处理。

接着，存储器接口利用生成的完整性检验值（ICV）生成密钥 Kicv_r1 生成撤消表的 ICV′，和执行与事先存储在撤消表中的正确 ICV 进行核对处

理（ICV′ = ICV? ）（S110）。ICV′的生成处理是通过根据上面参照图 14 所述的 DES 模式，利用初始值 IVicv-r1，和应用完整性检验值（ICV）生成密钥 Kicv-r1 的处理进行的。

在 ICV′ = ICV 成立的情况下（在 S111 中的“是”），判断撤消表是有效的，即没有被窜改，并且将其设置成对于诸如读出内容等之类的处理来说是可参考的状态，和把撤消表设置标志设置成 1（设置）（S112）。把撤消表存储在存储器接口内的存储器（例如，存储单元 321（参见图 4））中，并且，一旦发送／接收控制单元 306 从控制单元 205 接收到介质识别命令（参见图 2），就在已经设置的撤消表的介质标识符与已经安装到设备上的介质的介质标识符之间进行核对，和一旦发送／接收控制单元 306 从控制单元 205 接收到与内容的读出处理同时出现的标题设置命令，就在已经设置的撤消表中的内容标识符与作为读出对象的内容的内容标识符之间进行核对。

这样，在直接存取外部存储器等的存储器接口中建立起撤消表，并且，在建立之后，这种撤消表具有当安装介质和再现内容时在存储器接口上可不断使用的结构，因此，当使用内容时没有必要重复地执行从存储器中读出的处理，和可以有效地执行处理。

下面继续描述图 16 所示的流程图。在 ICV′≠ICV 成立（在 S111 中的“否”）的情况下，判断撤消表已经被窜改了，禁止内容基于表参考处理的处理，并且结束处理。由于上面处理结束了，把忙标志设置成 0。

另一方面，控制单元方把状态读出命令发送到存储器接口（S114），并且在忙标志是 0 的条件下（S115）保存撤消表设置标志（S116）。在判断撤消表没有被窜改的情况下，将要保存的撤消表设置标志设置成指示该表格已经被设置成有效的 1，否则，将其设置成 0。

（在识别介质时的处理）

接着，对识别介质时执行的处理，譬如，在把介质安装到设备上的情况下确认介质的有效性加密描述。如上所述，存在着两种类型的介质，即，不与设备进行相互验证处理的类型的介质 1、和与设备进行相互验证处理的类型的介质 2。一旦把每一种介质安装到设备上，设备就执行确认是否允许利用介质进行内容处理，具体地说，确认在撤消表中是否没有被登记成未授权介质的处理，在安装介质没有被列在撤消表中和被确认为可正当使用介质的条件下，把存储在介质中作为存取许可表的 BPT（块许可表）设置到存储器

接口中，并且执行使存储器能够参照 BPT 进行存取的处理。

首先，参照图 18 和图 19 描述在安装了介质 1 的情况下的介质确认处理。

图 18 和图 19 还在左边显示了图 2 所示的设备 200 的控制单元 205 的处理，和在右边显示了存储器接口单元 300 的处理。在开始处理那一时刻存储器接口单元的状态寄存器的状态是：忙标志：0（就绪）、介质 1 有效标志：0（无效）、和介质 1 设置标志：0（未设置）。

首先，控制单元识别安装到设备上的介质是否是介质 1（S201）。根据事先设置的基于介质形式的机械信息，或根据设备与介质之间的通信信息进行介质识别。一旦识别出这是介质 1，控制单元就把介质 1 识别命令发送到存储器接口（S202）。

一旦从控制单元接收到介质 1 识别命令（S203），存储器接口单元就把状态寄存器的忙标志设置成 1（忙）（S204），把有关介质 1 的标识符（ID）的读出命令发送到介质 1（S205），并接收（S206）。并且，在接收的介质 1 ID 与已经设置在撤消表中的撤消介质 1 的列表进行比对（S207）。正如上面针对图 16 所示的启动流程图所述的那样，在启动时，在存储器接口中建立起撤消表，并且，在建立之后，在安装介质和再现内容时在存储器接口上可不断使用它。

如果在列表中不存在与接收 ID 相匹配的 ID，那么，判断安装介质 1 不是作为撤消对象的介质，而是可正当使用的介质（在 S208 中的“是”），因此，把状态寄存器的介质 1 有效标志设置成 1（有效）（S209），并且把忙标志设置成 0（就绪）（S210）。如果在列表中存在与接收 ID 相匹配的 ID，那么，判断安装介质 1 是作为撤消对象的介质，不是可正当使用的介质，因此，不执行步骤 S209 中有效标志的设置处理，但在步骤 S210 中把忙标志设置成 0（就绪），然后，结束处理。

另一方面，在步骤 S211 中，控制单元方把状态读出命令发送到存储器接口，和在确认忙标志是 0（就绪）（S212）之后，只有在这个标志有效（标志：1）的情况下确定介质标志状态和继续处理，和在这个标志无效（标志：0）的情况下结束处理（在 S213 中的“否”）。

接着，流程转到图 19，控制单元把与介质 1 有关的文件分配表取出命令发送到存储器接口单元（S221），存储器接口把文件分配表存储在什么地方的扇区读出命令发送到介质 1（S222），从介质 1 接收文件分配表，和将

它发送到控制单元（S223）。

一旦接收到与存储在介质 1 中的数据有关的文件分配表（S224），控制单元就根据该表格执行块许可表（BPT）的读出处理（S225），并且把 BPT 设置命令和 BPT 发送到存储器接口（S226）。BPT 的设置处理只有在 BPT 有效的情况下才进行，并且，一旦 BPT 得到设置，就判断在内容处理，譬如，写来自介质的内容的处理等时是否可以参照 BPT，以块为单位进行擦除。以后再描述实际与 BPT 有关的数据写处理。

一旦从控制单元接收到块许可表（BPT）设置命令和 BPT，存储器接口就把状态寄存器的忙标志设置成 1（忙）（S228），并且生成用于 PBT 窜改检验的密钥 Kicv_bpt（S229）。

用于 BPT 窜改检验的完整性检验值（ICV）生成密钥 Kicv_bpt 是根据用于生成事先存储在设备内的 BPT 的 ICV 密钥的主密钥 MKicv_bpt、供生成 BPT 的 ICV 密钥时使用的初始值 IVicv_bpt、和包含介质 ID 的数据生成的。具体地说，这是根据完整性检验值（ICV）生成密钥 Kicv_bpt = DES（E，MKicv_bpt，mediaID^IVicv_bpt）生成的。这个方程的含义是根据介质 1 ID 与初始值（IVicv_bpt）的异或运算结果，利用主密钥 MKicv_bpt，在 DES 模式下进行加密处理。

接着，存储器接口利用生成的完整性检验值（ICV）生成密钥 Kicv_bpt 生成 BPT 的 ICV′，和与事先存储在 BPT 中的正确 ICV 值进行核对处理（ICV′ = ICV? ）（S230）。ICV′的生成处理是通过根据参照上面图 14 所述的 DES 模式，应用生成的完整性检验值（ICV）生成密钥 Kicv_bpt 和利用初始值 IVicv_bpt 的处理进行的。并且，根据包含介质的标识符（ID）的数据生成作为 BPT 的辅助信息存储的 ICV。因此，ICV 检验不仅起核实 BPT 的数据是否被窜改的作用，而且起核实 BPT 对于介质来说是否是唯一有效的，即，是否不是被复制到其它独立介质的 BPT 的作用。

在 ICV′ = ICV 成立的情况下（在 S231 中的“是”），判断存储在有效介质中的 BPT 是有效的，即没有被窜改，并且将其设置成对于内容处理等来说是可参考的状态，和把介质 1 设置标志设置成 1（设置）（S232）。在 ICV′≠ICV 成立（在 S231 中的“否”）的情况下，判断 BPT 已经被窜改了，禁止内容基于 BPT 参考处理的处理，并且结束处理。由于上面处理结束了，把忙标志设置成 0（S233）。

另一方面，控制单元方把状态读出命令发送到存储器接口（S234），并且在忙标志是0的条件下（在S235中的“是”）保存介质1设置标志（S236）。在判断该表格没有被窜改的情况下，将要保存的介质1设置标志设置成指示该表格已经被设置成有效的的1，否则，将其设置成0。

接着，参照图20和图21描述在安装了介质2时进行的确认处理。正如参照图2所述的那样，介质2是与设备进行相互验证的介质。

在图20中从S301到S304的步骤与介质1确认处理中的S201到S204相同，因此，略去不述。

在步骤305中，存储器接口与介质2进行相互验证处理。

图22显示了利用共享密钥加密方法的相互验证方法（ISO/IEC 9798-2）的处理序列。在图22中，DES用作这个共享密钥加密方法，但是，也可以使用其它方法，只要它们是共享密钥加密方法即可。在图22中，首先，B生成64-位随机数Rb，并且把Rb和它自身的ID，即ID（b）发送到A。一旦接收到它们，A就生成新的64-位随机数Ra，并且按照Ra、Rb、和ID（b）的次序，在DES CBC模式下，利用密钥Kab加密数据，将其返回到B。请注意，密钥Kab是A和B共享的秘密密钥和验证密钥。在利用，例如，DES的处理中，在DES CBC模式下利用密钥Kab的加密处理计算初始值和Ra的异或，利用密钥Kab在DES加密单元上进行加密，生成密文（ciphertext）E1，然后，计算密文E1和Rb的异或，利用密钥Kab在DES加密单元上进行加密，生成密文E2，进一步计算密文E2和ID（B）的异或，利用密钥Kab在DES加密单元上进行加密，生成密文E3，从而生成发送数据（Token-AB）。

一旦接收到它，B利用也作为共享秘密密钥的、存储在每个记录设备中的密钥Kab（验证密钥）解密接收数据。至于解密接收数据的方法，首先，利用验证密钥Kab解密密文E1，和获取它与初始值的异或，从而获得随机数Ra。接着，利用验证密钥Kab解密密文E2，获取所得的结果和E1的异或，从而获得Rb。最后，利用验证密钥Kab解密密文E3，获取所得的结果和E2的异或，从而获得ID（b）。在如此获得的Ra、Rb、和ID（b）当中，对Rb和ID（b）是否与B已经发送的Rb和ID（b）相匹配加以核实。在这个核实得到肯定的情况下，B认为A是有效的。

接着，B生成含有随机数的、在下面的验证中要使用的会话密钥（Kses）。然后，按照Rb、Ra、和Kses的次序，利用验证密钥Kab，在DES CBC模式

下进行加密，并且将其返回到 A。

一旦接收到它，A 就利用验证密钥 Kab 解密接收数据。接收数据的解密方法与 B 的解密处理相同。在如此获得的 Rb、Ra、和 Kses 当中，对 Rb 和 Ra 是否与 A 已经发送的 Rb 和 Ra 相匹配加以核实。在这个核实得到肯定的情况下，A 认为 B 是有效的。在相互验证之后，会话密钥 Kses 用作验证之后的秘密通信的共享密钥。

如果在核实接收数据时发现不法行为或不匹配，那么，就认为相互验证已经失败了，随后，禁止相互数据通信处理。

图 23 和图 24 显示了在根据本发明的设备与介质之间进行相互验证和密钥（会话密钥）共享处理的流程图。在图 23 和图 24 中左边是设备的存储器接口，和右边是在介质 2 的控制器上的处理。

首先，介质 2 控制器生成随机数 Ra（S401），并且将随机数 Ra 和作为它自身 ID 的介质 2 ID 发送到设备存储器接口（S402）。一旦接收到它们（S403），设备存储器接口通过把它拥有的验证密钥生成主密钥 MKake 应用于接收的介质 2 ID 和初始值（IV_ake）的异或，进行 DES 加密处理，从而生成验证密钥 Kake（S404）。并且，设备存储器接口重新生成随机数 Rb（S405），计算初始值 IV/auth 和 Rb 的异或，利用密钥 Kake 加密它，生成密文 E1，随后，计算 E1 和 Ra 的异或，利用密钥 Kake 加密它，生成密文 E2，进一步，计算 E2 和介质 2 ID 的异或，利用密钥 Kake 加密它，生成密文 E3（S406），把生成的数据 E1||E2||E3 发送到介质 2 控制器（S407）。请注意，[||]的含义是数据的连接。

一旦接收到它（S408），介质 2 控制器就利用验证密钥 Kake 解密接收数据（S409）。至于接收数据的解密方法，利用验证密钥 Kake 解密密文 E1，和获取它与初始值的异或，从而获得随机数 Rb′。接着，利用验证密钥 Kake 解密密文 E2，获取所得的结果和 E1 的异或，从而获得 Ra′。最后，利用验证密钥 Kake 解密密文 E3，获取所得的结果和 E2 的异或，从而获得介质 2 ID′。在如此获得的 Ra′、Rb′、和介质 2 ID′当中，对 Ra′和介质 2 ID′是否与介质 2 已经发送的 Ra 和介质 2 ID 相匹配加以核实（S410 和 S411）。在这个核实得到肯定的情况下，介质 2 认为设备是有效的。在 Ra′和介质 2 ID′不与发送数据相匹配的情况下，认为相互验证已经失败了（S413），取消随后的数据通信。

接着，介质 2 控制器生成随机数，用作在下面的验证中要使用的会话密钥（Kses）。然后，在图 24 的步骤 S421 中，按照 Ra、Rb、和 Kses 的次序，利用验证密钥 Kake，在 DES CBC 模式下进行加密，并且将其发送到设备存储器接口（S422）。

一旦接收到它（S423），设备存储器接口就利用验证密钥 Kake 解密接收数据。在如此获得的 Ra"、Rb"、和 Kses 当中，对 Ra"和 Rb"是否与设备已经发送的 Ra 和 Rb 相匹配加以核实（S425 和 S426）。在这个核实得到肯定的情况下，设备认为介质 2 是有效的（S427）。在相互验证之后，共享会话密钥 Kses（S429），和会话密钥 Kses 用作验证之后的秘密通信的共享密钥。在 Ra"和 Rb"不与发送数据相匹配的情况下，就认为相互验证已经失败了，取消随后的数据通信。

返回到图 20，继续描述介质 2 的识别处理。在步骤 305 中，进行上述相互验证和密钥共享处理，并且，一旦在步骤 S306 中确认相互验证已经成功了，就在在相互验证处理期间接收的介质 2 的 ID 与已经设置的撤消表中的撤消介质 2 的列表之间进行比对（S307）。

如果在列表中不存在与接收 ID 相匹配的 ID，那么，判断安装介质 2 不是作为撤消对象的介质，而是可正当使用的介质（在 S308 中的“否”），因此，把状态寄存器的介质 2 有效标志设置成 1（有效）（S309），并且把忙标志设置成 0（就绪）（S310）。如果在列表中存在与接收 ID 相匹配的 ID（在 S308 中的“是”），那么，判断安装介质 2 是作为撤消对象的介质，不是可正当使用的介质，因此，不执行步骤 S309 中有效标志的设置处理，但在步骤 S310 中把忙标志设置成 0（就绪），然后，结束处理。

另一方面，在步骤 S311 中，控制单元方把状态读出命令发送到存储器接口，和在确认忙标志是 0（就绪）（S312）之后，只有在这个标志有效（标志：1）的情况下确定介质标志状态和继续处理，和在这个标志无效（标志：0）的情况下结束处理（在 S313 中的“否”）。

接着，流程转到图 21，控制单元把与介质 2 有关的文件分配表取出命令发送到存储器接口单元（S321），存储器接口把存储了文件分配表的扇区读出命令发送到介质 2（S322），从介质 2 接收文件分配表，和将它发送到控制单元（S323）。

一旦接收到与存储在介质 2 中的数据有关的文件分配表（S324），控制

单元就根据该表格执行块许可表（BPT）的读出处理（S325），并且把 BPT 设置命令和 BPT 发送到存储器接口（S326）。BPT 的设置处理只有在 BPT 有效的情况下才进行，并且，一旦 BPT 得到设置，就判断在内容处理，譬如，写来自介质的内容的处理时是否可以参照 BPT 以块为单位进行擦除。以后再描述实际与 BPT 有关的数据写处理。

一旦从控制单元接收到块许可表（BPT）设置命令和 BPT（S327），存储器接口就把状态寄存器的忙标志设置成 1（忙）（S328），并且生成用于 PBT 窜改检验的完整性检验值（ICV）生成密钥 Kicv_bpt（S329）。

用于 BPT 窜改检验的完整性检验值（ICV）生成密钥 Kicv_bpt 是根据用于生成事先存储在设备内的 BPT 的 ICV 密钥的主密钥 MKicv_bpt、供生成 BPT 的 ICV 密钥时使用的初始值 IVicv_bpt、和介质 2 ID 生成的。具体地说，这是根据完整性检验值（ICV）生成密钥 Kicv_bpt = DES（E，MKicv_bpt，mediaID^IVicv_bpt）生成的。这个方程的含义是通过对介质 2 ID 与初始值（IVicv_bpt）进行异或运算，利用主密钥 MKicv_bpt，在 DES 模式下进行加密处理。

接着，存储器接口利用生成的完整性检验值（ICV）生成密钥 Kicv_bpt 生成 BPT 的 ICV′，和与事先存储在 BPT 中的正确 ICV 值进行核对处理（ICV′ = ICV? ）（S330）。ICV′的生成处理是通过根据参照上面图 14 所述的 DES 模式，应用生成的完整性检验值（ICV）生成密钥 Kicv_bpt 和利用初始值 IVicv_bpt 的处理进行的。并且，根据包含介质 2 ID 的数据生成作为 BPT 的辅助信息存储的 ICV。因此，ICV 检验不仅起核实 BPT 的数据是否被窜改的作用，而且起核实 BPT 对于介质来说是否是唯一有效的，即，是否不是被复制到其它独立介质的 BPT 的作用。

在 ICV′ = ICV 成立的情况下（在 S331 中的“是”），判断 BPT 是有效的，即没有被窜改，和存储在有效介质中，并且将其设置成对于内容处理来说是可参考的状态，和把介质 2 设置标志设置成 1（设置）（S332）。在 ICV′≠ICV 成立（在 S331 中的“否”）的情况下，判断 BPT 已经被窜改了，禁止内容基于 BPT 参考处理的处理，并且结束处理。由于上面处理结束了，把忙标志设置成 0（S333）。

另一方面，控制单元方把状态读出命令发送到存储器接口（S334），并且在忙标志是 0 的条件下（在 S335 中的“是”）保存介质 2 设置标志（S336）。

在判断该 BPT 没有被窜改的情况下，将要保存的介质 2 设置标志设置成指示该表格已经被设置成有效的的 1，否则，将其设置成 0。

（数据文件读出处理）

接着，参照图 25 所示的流程图，描述读出数据文件的处理。数据文件包括音乐数据、图像数据、和诸如内容数据文件，以及上述撤消表之类的其它数据。图 25 所示的流程图是读出存储在任何内部存储器或外部存储器（介质 1 和介质 2）中的数据文件通用的处理流程。在图 25 中，左边是设备的控制单元中的处理，右边是在设备的存储器接口中的处理。

首先，控制单元从文件分配表（参见图 17）中获取要读出的数据的扇区地址（S（1）到 S（k））（S501），并且，把获得的扇区 S（i）读出命令依次发送到存储器接口（S502，S503）。一旦接收到扇区 S（i）读出命令（S504），存储器接口就把忙标志设置成 1（忙）（S505），判断接收的扇区 S（i）是内部存储器还是外部存储器（S506），并且，在是内部存储器的情况下，判断介质 1 或介质 2 的设置标志是否是 1（指示介质被设置成有效的）（S507），和在设置标志是 1 的情况下，进一步参考块许可表（BPT），判断 BPT 是否把这个作为读出对象的扇区 S（i）设置成允许读出的块（S508）。在存在设置在 BPT 中的读出许可块的情况下，从外部存储器中读出在这个扇区上的数据（S509）。

现在，如果要读出的数据是不受 BPT 管理的内部存储器中的数据，那么，跳过步骤 S507 和 S508。如果在步骤 S507 和 S508 中作出的判断是“否”，即，如果存储这个扇区 S（i）的介质的设置标志不是 1，或者，如果在 BPT 中对于扇区 S（i）没有设置成读出许可，那么，流程转到步骤 S513，把读出成功标志设置成 0，表示读出错误。

如果在步骤 S506 到 S508 的判断块中判断目标扇区 S（i）的读出是可执行的，那么，从存储器中读出这个扇区，并且执行基于与扇区相对应地设置的冗余部分中的纠错码的纠错处理（S510），确认纠错是否已经取得成功（S511），把读出成功标志设置成 1（成功），把读出结果存储在缓冲器中（S512），和把忙标志设置成 0（就绪）（S513）。在纠错失败的情况下，把读出成功标志设置成 0（失败）（S513），然后，结束处理。

此外，在步骤 S515 到 S520 中，控制单元读出存储器接口的状态，并且，在忙标志是 0 的状态下，和在读出成功标志是 1 的条件下，从缓冲器中提取

读出数据和保存它，然后，依次递增地址，重复执行从缓冲器中依次提取数据和保存它的处理，和在保存了作为读出对象的所有扇区之后，该文件由已经读出的所有扇区构成，然后，结束处理。

（文件写入处理）

接着，参照图 26 所示的流程图描述写入数据文件的处理。图 26 所示的流程图是把数据文件写入任何内部存储器或外部存储器（介质 1 和介质 2）通用的处理流程。在图 26 中，左边是设备的控制单元，右边是设备的存储器接口。

首先，控制单元把作为写入对象的文件划分成若干个扇区（S601）。假设分数据为 D（1）到 D（k）。控制单元接着为每个数据 D（i）设置写扇区 S（i），并且把扇区 S（i）写入命令和数据 D（i）依次发送到存储器接口（S602 到 S604）。一旦接收到扇区 S（i）写入命令（S605），存储器接口就把忙标志设置成 1（忙）（S606），判断接收扇区 S（i）是内部存储器还是外部存储器（S607），并且，在是外部存储器的情况下，判断介质 1 或介质 2 的设置标志是否是 1（指示该介质被设置成有效的）（S608），和在设置标志是 1 的情况下，进一步参考块许可表（BPT），判断 BPT 是否已经把作为写对象的扇区 S（i）设置成写入许可块（S609）。如果在 BPT 中存在作为写入许可块的设置，那么，生成与扇区相对应地设置的纠错码（S610），把含有纠错码的冗余部分和数据 S（i）写入扇区 S（i）和数据 D（i）中（S611），把写入成功标志设置成 1（成功）（S612），和把忙标志设置成 0（就绪）（S614）。

现在，如果要写入的数据正在经历写入不受 BPT 管理的内部存储器的写入处理，那么，跳过步骤 S608 和 S609。如果在步骤 S608 和 S609 中作出的判断是“否”，即，如果介质的设置标志不是 1，或者，如果在 BPT 中没有把扇区 S（i）设置成写入许可，那么，流程转到步骤 S613，把写入成功标志设置成 0，表示读出错误。

此外，在步骤 S616 到 S620 中，读出存储器接口的状态，在忙标志是 0 的情况下，依次递增地址，并且，在写入成功标志是 1 的条件下，把写入数据依次发送到存储器接口。在结束所有处理之后，执行文件分配表的更新处理（S621），把更新的文件分配表与更新命令一道发送到存储器接口（S622），并且，存储器接口根据命令执行写入文件分配表的处理（S623）。

[应用与扇区位置相对应的加密密钥的加密处理]

接着，对应用与扇区位置相对应的加密密钥的加密处理加以描述。存在着为了保护版权等而对内容部分进行加密的情况，但是，在用单个加密密钥加密全部内容部分的情况下，这意味着大量密文是在单个密钥下生成的，因此，增加了易受攻击的危险性。一般来说，最好尽可能多地把内容部分划分成若干个块，用不同的密钥加密每一块。对于用当前系统加密内容来说，可以把扇区当作最小单元，但是，在把密钥保存在标题区中的情况下，对于每个扇区，需要 8 个字节（在 DES 的情况下）或 16 个字节（在三重 DES 的情况下）的密钥信息，因此，标题尺寸变得非常大，这缩小了有限存储区中的数据区，在实践中是不合需要的。此外，应用把加密扇区的密钥存储在那个扇区的数据区中的方法不影响标题尺寸，但是，由于不能把数据放置在密钥区中，数据尺寸缩减了，并且，在控制单元方拥有文件系统的系统的情况中，需要对文件系统本身作较大改动。

因此，根据本发明，把与介质的每个块中 M 个扇区相对应的 M 段密钥信息存储在作为上述内容属性信息的一个保密标题（参见图 7）中，和把这些加密信息用作每个扇区的加密密钥（参见图 8）。在图 7 所示的保密标题内 Kc_Encrypted0 到 Kc_Encrypted31 表示 32 个加密密钥 Kc。请注意，[Encrypted]表示每个密钥 Kc 被加密和存储了。其结构是这样的，根据扇区在块中的位置，从这些众多密钥中选择密钥，用作与扇区相对应的加密密钥。

图 27 显示了说明作为内容的标题信息的、与内容相对应地生成的保密标题中的密钥存储结构，和存储的密钥与存储器内作为密钥应用对象的扇区之间的相关性的图形。图 27（a）是以简化方式说明在前面参照图 7 所述的保密标题内的密钥存储结构的图形。从 Kc（0）到 Kc（M-1）的 M 个密钥（内容密钥）存储在图 7（a）所示的保密标题中。除了密钥之外，诸如版本、内容类型之类的各种信息也存储在标题中，并且，还存储了用于标题信息窜改检验的 ICV。

M 个内容密钥的每一个与扇区的每一个相关联，用于加密，例如，图 27（b）所示的要存储在扇区中的数据。正如前面参照图 3 所示的那样，按块递增方式进行擦除的闪速存储器含有如图 27（b）所示的按递增方式划分成块的数据存储区，其中每个块进一步被划分成多个扇区。例如，把密钥 Kc（0）用作加密要存储在存储器中这些块的扇区 0 中的数据的密钥，把密钥 Kc（s）用作加密要存储在存储器中这些块的扇区 s 中的数据的密钥。并且，

把密钥 Kc（M-1）用作加密要存储在存储器中这些块的扇区 M-1 中的数据的密钥。

因此，通过应用与扇区相对应的不同加密密钥来存储数据（例如，内容），加强了存储数据的保密性。也就是说，尽管在利用单个密钥加密整个内容的情况中，可以通过一个泄密密钥加密整个内容，但是，借助于本发明的结构，不可能根据单个泄密密钥来解密整个数据。

例如，利用单个加密密钥进行 DES 加密处理的单重 DES 用于加密算法。此外，应用把两个或更多个密钥用于加密的三重 DES 的加密结构可以用于取代单重 DES。

图 28 显示了三重 DES 的详细结构例子。如图 28（a）和（b）所示，存在着如下两种代表三重 DES 结构的不同形式。图 28（a）显示了利用 2 个加密密钥的例子，其中按照用密钥 1 进行加密处理，用密钥 2 进行解密处理，并且用密钥 1 进行加密处理的次序进行处理。两种密钥是按照 K1、K2、和 K1 的次序加以使用的。图 28（b）显示了利用 3 个加密密钥的例子，其中按照用密钥 1 进行加密处理，用密钥 2 进行加密处理，并且用密钥 3 进行加密处理的次序进行处理，三次的每一次都是进行加密处理。三种密钥是按照 K1、K2、和 K3 的次序加以使用的。通过连续多重处理的结构，可以把保密程度提高到高于单重 DES 的保密程度。

图 29 说明了把两个不同加密密钥的一对应用于在存储在存储器中的数据的每个扇区，进行通过三重 DES 的加密处理的结构例子。如图 29 所示，利用密钥 Kc（0）和 Kc（1）的两个密钥对每个块的扇区 0 进行三重 DES 加密，利用密钥 Kc（s）和 Kc（s+1）的两个密钥对每个块的扇区 s 进行三重 DES 加密，和利用密钥 Kc（M-1）和 Kc（0）的两个密钥对每个块的扇区 M-1 进行三重 DES 加密。对于这种情况，要存储在标题中的密钥的个数也是 M，因此，可以加强保密性，而无需增加如图 27（a）所示存储的密钥的个数。

并且，基于不同形式的数据加密结构例子显示在图 30 中。图 30 是利用 2 个密钥进行三重 DES 加密的形式，其中，在存储器的每个块中两个相继扇区组成的区域被当作一个加密块。如图 30 所示，利用密钥 Kc（0）和 Kc（1）的两个密钥对每个块的扇区 0 和扇区 1 进行三重 DES 加密，利用密钥 Kc（2s）和 Kc（2s+1）的两个密钥对每个块的扇区 2s 和扇区 2s+1 进行三重 DES 加密，和利用密钥 Kc（M-2）和 Kc（M-1）的两个密钥对每个块的扇区 M-2 和

扇区 M-1 进行三重 DES 加密。因此，通过把相同的加密处理应用于多个扇区，可以减轻加密处理或解密处理的处理负担。

除了图 27、图 29 和图 30 所示的例子之外，还可以构造出各种结构作为利用从存储在标题中的多个密钥中选择的密钥对每个扇区进行加密的结构。例如，在图 27、图 29 和图 30 中，该结构拥有存储在标题中的、个数与扇区数相同的密钥，但是，在扇区数例如是 M 的情况下，可以使用存储密钥的个数是 N（其中 N < M）的结构，以便扇区 0 到扇区 s 用相同的密钥加密，以此类推。或者，可以构造出存储密钥的个数是 L（其中 L > M）的结构，以便对每个扇区应用具有完全不同的多个密钥组的三重 DES。

[按扇区递增方式加入完整性检验值（ICV）的结构]

接着，描述按扇区递增方式加入完整性检验值（ICV）的结构。在确认了在多个扇区上构成的数据的有效性的情况下，一般来说，把上述完整性检验值（ICV）加入整个内容数据的末端等位置的结构是常见的。对于这种把 ICV 加入整个数据中的结构，按照构成数据的扇区的递增方式不能确认有效性。

此外，在存储 ICV 的情况中，把 ICV 放置在与作为实际数据的内容的存储区相同的区域中使可用作数据部分的区域减少 ICV 所占据的那么多。如果每个扇区的 ICV 都要被放在每个扇区中的数据中，那么，需要把实际使用的数据与 ICV 分开和提取实际使用的数据的处理，即，移去在已经读出的数据部分的扇区中的 ICV 的处理，和把提取扇区内的数据的多个扇区链接起来的处理，对于执行按数据部分递增读出数据的处理的设备的文件系统，有必要把文件系统重新构造成能执行这样的处理。并且，在控制单元上进行 ICV 检验使得控制单元的处理负担过重。

根据本发明的数据处理设备，把 ICV 设置在每个扇区中，以便能够对每个扇区进行数据窜改检验，并且，不把 ICV 设置在实际的数据区中，而是把 ICV 放置在事先设置成设备的文件系统不去读的区域的冗余部分中。借助于把 ICV 放置在冗余部分中的结构，无需把 ICV 放置在数据内，因此，可以使用数据部分的更多区域。此外，把 ICV 放置在冗余部分中轻而易举地消除了将数据部分与 ICV 分开的必要性，和省去了把数据链接起来，以便保持读出数据的连续性的处理。

在读数据时，在存储器接口单元 300（参见图 2）上对每个扇区进行 ICV

检验处理，并且，在判断存在窜改，和数据是无效的情况下，不进行到控制单元 205（参见图 2）的传送。此外，在写数据时，在存储器接口单元 300 上对每个扇区计算 ICV，并且，进行将其写入冗余部分的处理。

此外，通过在保密标题中进行描述规定是否把 ICV 加入每个扇区中。对于这种结构，如图 7 中保密标题结构的描述所示，保密标题内的 ICV 标志拥有与一个块中扇区的个数（32 个扇区）一样多的标志，用于指示把 ICV 加入／不加入一个块内的每个扇区中。例如，设置 0：没有 ICV，1：加入 ICV。

图 31 说明了数据使用部分和冗余部分结构。如图 31（a）所示，存储在存储器（闪速存储器）中的数据被划分成拥有多个扇区的按块递增区域来存储。如图（b）所示，每个扇区例如由 512 个字节或 1024 个字节可由设备的文件系统读取作为实际数据（例如，内容）的数据使用部分、和存储诸如 ECC（纠错码）之类不可由文件系统读取的信息的冗余部分构成。

这个冗余部分的容量预定为例如 16 个字节或 20 个字节的区域，设备的文件系统把这个冗余部分识别为非数据区，在数据（内容）读处理过程中是不能读它的。一般来说，存储在冗余部分中的 ECC 不占用整个冗余部分，在冗余部分中还存在未使用区（备用区）。扇区的完整性检验值（ICV）就存储在这个备用区中。

如图 31（c）所示，可以使在把 ICV 存储在冗余部分中的情况下设备的文件系统对数据部分的链接处理与简单链接只存储纯粹用作数据的数据的数据部分的传统数据链接处理相同。这样，设备的文件系统必须做的全部工作是简单链接除了冗余部分之外的数据部分的区域，因此，一点也不需要任何新的处理。

根据本发明的结构，可以按照由多个扇区组成的数据的扇区的递增方式核实数据的有效性。此外，把用于窜改检验的 ICV 放置在冗余部分中使可以用于数据的数据区按原样得以使用。此外，只有根据 ICV 检验结果被判断为正当（没有被窜改）的扇区才被发送到控制单元。此外，ICV 检验是在存储器接口上进行的，因此，具有诸如不对控制单元增加负担之类的优点。

[通过介质内的个别密钥进行的内容密钥存储处理]

接着，描述有关通过介质内的个别密钥保存内容密钥的处理的结构。如参照图 7 所述，加密用作与扇区相对应的加密密钥的多个内容密钥（Kc_Encryptedxx）、和一个内容完整性检验值生成密钥（Kicv_Encrypted），将

它们存储在与内容相对应地构成的保密标题中。

加密这些密钥的形式之一是通过事先存储在设备的存储器接口的存储单元 321（参见图 4）中的分配密钥 Kdist 加密这些密钥和存储这些密钥的结构。例如，Kc-Encrypted0 = Enc（Kdist，Kc（0））。这里，Enc（a，b）表示数据是由 a 加密的 b。这样，利用设备的分配密钥 Kdist 加密密钥和将其存储在保密标题中的结构是一种结构。

并且，对于介质 2，即，含有加密处理单元和通过与设备进行相互验证来执行内容处理的介质，存在着利用介质 2 的唯一密钥加密与存储在介质 2 中的内容相关的内容密钥、和 ICV 生成密钥的形式。下面描述存储利用介质 2 的唯一密钥，在这种情况中，介质 2 存储密钥 Ksto，加密的内容密钥和内容 ICV 生成密钥的处理。

如图 2 所示，介质 2 存储密钥 Ksto 存储在介质 2，即 230 的介质 2 控制器 231 的内部存储器 235 中。因此，在介质 2 方执行利用介质 2 存储密钥 Ksto 对内容密钥和 ICV 生成密钥的加密处理和解密处理。在安装了介质 2 的设备使用介质 2 中的内容时，如果要执行内容密钥和 ICV 生成密钥的获得，或到保密标题的存储处理，那么，需要在介质 2 方执行密钥的加密和解密处理。对于根据本发明的数据处理设备，已经能够利用 CBC（密码块链接）模式处理它们。

图 32 说明了在 CBC 模式下密钥的加密处理结构。这种加密处理是在介质 2 的加密处理单元 236（参见图 2）中执行的。对存储在内部存储器 235 中的初始值 IV-keys 和内容完整性检验值生成密钥 Kicv-cont 进行异或运算，让所得的结果经过应用存储在介质 2 的内部存储器 235 中的存储密钥 Ksto 的 DES 加密，和把结果存储在标题中作为 Kicv-cont Encrypted（加密的 Kicv-cont）。并且，对 Kicv-cont Encrypted 和与扇区（0）相对应的扇区对应内容密钥 Kc（0）进行异或运算，让所得的结果经过应用存储在介质 2 的内部存储器 235 中的存储密钥 Ksto 的 DES 加密，和把结果存储在标题中作为 Kc（0）Encrypted（加密的 Kc（0）），它是一个加密内容密钥。并且，对 Kc（0）Encrypted 和与扇区（1）相对应的扇区对应内容密钥 Kc（1）进行异或运算，让所得的结果经过应用存储密钥 Ksto 的 DES 加密，和把结果取作 Kc（1）Encrypted（加密的 Kc（1））。随后，重复执行这个处理，从而获得用于标题存储的密钥数据。

接着，在 CBC 模式下的密钥解密处理结构显示在图 33 中。这个解密处理是在介质 2 的加密处理单元 236（参见图 2）中执行的。首先，对 Kc（0）Encrypted 进行应用存储在介质 2 的内部存储器 235 中的存储密钥 Ksto 的 DES 解密处理，所得的结果与存储在内部存储器 235 中的初始值 IV_keys 的异或运算，输出与扇区（0）相对应的扇区对应内容密钥 Kc（0）。并且，对 Kc（1）Encrypted 进行应用存储密钥 Ksto 的 DES 解密处理，所得的结果与内容密钥 Kc（0）Encrypted 的异或运算，输出与扇区（1）相对应的扇区对应内容密钥 Kc（1）。随后重复这些处理，从而获得内容密钥。现在，虽然附图显示了只有内容密钥是输出数据的例子，但是，相同的处理可以应用于内容完整性检验值生成密钥（Kicv_Encrypted），和可以从加密内容完整性检验值生成密钥（Kicv_ Encrypted）中生成内容完整性检验值生成密钥（Kicv）。

在许多情况中，上述扇区对应内容密钥 Kc（xx）或内容完整性检验值生成密钥（Kicv）的加密和解密处理是根据来自安装了介质 2 的设备的命令执行的。在这种情况中，在设备与介质 2 之间进行上述相互验证，在相互验证处理已经被确立的条件下进行内容的诸如再现、存储等之类的各种处理，并且执行上述内容密钥加密和解密处理作为一系列内容处理之一。如果在设备与介质 2 之间传送解密密钥（例如，内容密钥 Kc（xx）），那么，这是用在进行相互验证时生成的会话密钥 Kses 加密的。应用 CBC 模式也可以加强利用这个会话密钥 Kses 进行加密和解密处理的保密性。

图 34 说明了在介质 2 中，在 DES-CBC 模式下解密存储在保密标题中的密钥，并且在应用会话密钥 Kses 的 DES-CBC 模式下加密解密密钥数据的处理结构。图 34 的上部是与图 33 相同的结构，其中把从保密标题中提取的加密内容密钥依次输入到 DES 解密单元，在 DES 解密单元上应用介质 2 的存储密钥 Ksto 进行解密处理，在输出结果与初始值或输入数据串中的旧数据之间进行异或运算，从而，作为输出结果，获得内容密钥。

在应用与设备进行相互验证时生成的会话密钥 Kses 的 DES-CBC 模式下，再对输出结果进行加密处理。把如此获得的 SE0 到 SEM-1: Kc（0）Encrypted 到 Kc（M-1）Encrypted 传送到该设备。在设备方，对 Kc（0）Encrypted 到 Kc(M-1)Encrypted 进行在应用与介质 2 进行相互验证时生成的会话密钥 Kses 的、以与图 33 所使用相同的方式的 DES-CBC 模式下的解密处理，从而，能够获得内容密钥 K（c）。现在，虽然附图说明了只有内容密钥是处理数据的

例子，但是，可以按照相同的方式把内容完整性检验值生成密钥（Kicv-Encrypted）取作处理数据。

[加密数据读出处理]

下面参照图 35 所示的流程图描述从介质中读出加密数据的处理的细节。现在，数据加密形式包括如上所述利用不同密钥对每个扇区进行加密的形式、和利用单个密钥加密整个内容的形式，这些形式要根据标题信息来判断。在图 35 所示的流程图中，左边是在设备的控制单元上的处理，右边是在设备的存储器接口上的处理。

首先，控制单元读出作为读出对象的内容的标题文件（S701）。这个处理作为如上所述的、图 25 所示的文件读出处理之后的处理来执行。接着，把标题设置命令和读出的标题文件发送到存储器接口（S702）。

一旦接收到标题设置命令（S703），存储器接口就把忙标志设置成 1（忙）（S704），和核实标题的完整性检验值（ICV）（S705）。标题的 ICV 核实是通过如下处理进行的，在前面参照图 14 所述的 ICV 生成处理中，把保密标题核实值生成密钥 Kicv-sh 和初始值 IVsh 用于输入标题结构数据，生成 ICV′，然后，在生成的 ICV′与事先存储在标题中的 ICV 之间进行核对。

一旦通过核实判断标题没有被窜改（S706），就对标题中的有效撤消表版本是否不是 0 进行检验（S707）。例如，在把已经生成的和存储在自身设备中的内容存储在存储器中的情况下，进行把撤消表版本设置成 0 和在再现处理时不参考撤消表的处理。

在撤消表版本是 0 的情况下，无需参考撤消表，因此，流程转到步骤 S710。在版本不是 0 的情况下，对当前设置的撤消表的版本是否不旧于标题中的版本进行检验（S708），和在设置撤消表的版本旧于标题中的版本的情况下，流程转到步骤 S713，在步骤 S713 中，把标题设置成功标志设置成 0（失败），然后，结束处理。在设置撤消表的版本不旧于标题中的版本的情况下，流程转到步骤 S709，参考撤消表，判断是否存在作为读出对象的内容 ID。在存在的情况下，在步骤 713 中把标题设置成功标志设置成 0（失败），表示禁止读出，然后，结束处理。

在作为读出对象的内容 ID 没有被记录在撤消表中的情况下，流程转到步骤 S710，根据标题信息解密加密的内容密钥 Kc 和内容完整性检验值生成密钥 Kicv-cont。现在，如前面参照图 16 所示的启动流程所述的那样，在

启动时，在存储器接口中建立起撤消表，并且，在建立之后，在安装介质和再现内容时，在存储器接口上可不断使用它。

首先，如参照图 7 和其它附图所述，加密多个内容密钥 Kc(0)到 Kc(M-1)，将它们存储在保密标题中，作为如上所述要应用于每个扇区的加密密钥。此外，还加密和存储用于生成内容的完整性检验值（ICV）的内容完整性检验值生成密钥 Kicv_cont。

在解密内容之前，需要进行解密内容完整性检验值生成密钥 Kicv_cont 和执行内容的窜改检验的处理，并且，有必要进行解密内容密钥 Kc（0）到 Kc（M-1）的处理。

图 37 显示了加密内容密钥 Kc 和内容完整性检验值生成密钥 Kicv_cont 的解密处理流程。沿着图 37 所示的步骤进行描述。图 37 中处理是在设备的存储器接口方处理的。是在图 4 的加密处理单元 320 中执行的。

首先，选择加密内容完整性检验值生成密钥 Kicv_cont 作为解密对象（S801），接着，对标题中加密格式类型字段是否被设置成 0 加以判断（S802）。在加密格式是 0 的情况下，数据结构具有整个内容与扇区无关的加密形式，和在加密格式类型字段被设置成 1 的情况下，这是一种上述参照图 27 和其它附图把加密解密用于递增扇区的方法。在把加密解密用于递增扇区的方法的情况下，流程转到步骤 803，并且，把为每个扇区设置的加密内容密钥（Kc_Encrypted0 到 Kc_Encrypted31）设置成解密对象。

如果在步骤 S802 中判断加密格式类型字段是 0，那么，在步骤 S804 中进一步检验标题中加密算法字段，并且，对这是 1（三重 DES）还是 0（单重 DES）作出判断。如果是单重 DES，那么，在步骤 S805 中，只把一个加密内容密钥（Kc_Encrypted0）加入解密对象中；如果是三重 DES，那么，在步骤 S806 中，把多个加密内容密钥（Kc_Encrypted0，1）加入解密对象中。

接着，在步骤 S807 中，检验标题中内容类型字段的设置，并且，在设置不是 2 或 3（介质 2 的存储内容）的情况下，在步骤 808 中，把存储在存储单元 321（参见图 4）中的分配密钥 Kdist 用于解密作为解密对象的数据，即，加密内容完整性检验值生成密钥 Kicv_cont、和一个或多个内容密钥。

在设置是 2 或 3（介质 2 的存储内容）的情况下，在步骤 809 中，把介质 2 的存储密钥 Ksto（CBC 模式）用于解密作为解密对象的数据，即，加密内容完整性检验值生成密钥 Kicv_cont、和一个或多个内容密钥。这个解密

处理的细节已经参照 32、图 33 和图 34 作了描述。

下面参照图 38 描述通过介质 2 的存储密钥解密加密内容完整性检验值生成密钥 Kicv_cont 和一个或多个内容密钥的解密处理。在图 38 所示的流程图中，左边表示设备的存储器接口的处理，右边表示介质 2（参见图 2）的控制器上的处理。

首先，存储器接口把作为解密对象的数据设置成 K（0）到 K（n-1）（加密内容完整性检验值生成密钥 Kicv_cont 和一个或多个内容密钥）（S1001），把 CBC 解密初始化命令发送到介质 2 控制器（S1003），和介质 2 控制器把 IV_keys 设置到寄存器中（S1005）。随后，存储器接口依次发送密钥（S1004），和介质 2 控制器接收作为解密对象的数据 K（i）（S1006）。

接着，介质 2 控制器针对作为解密对象的接收数据 K（i），利用介质 2 的这个存储密钥 Ksto，通过 CBC 模式进行解密处理（S1007），和获取解密的密钥数据（例如，与多个扇区相对应的内容密钥）（S1008）。接着，介质 2 控制器针对解密的密钥数据流，利用与设备相互验证时生成的会话密钥，在 CBC 模式下，进行加密处理，生成数据串 K′（i），和把结果发送到该设备（S1009）。步骤 S1007 到 S1009 的处理是根据前面参照图 34 所述的、在 DES-CBC 模式下的处理进行的。

该设备的存储器接口依次接收 K′（i），并且，在确认已经接收到所有数据之后，把 CBC 结束命令发送到介质 2 控制器。一旦接收到 CBC 结束命令，介质 2 控制器就清除寄存器（S1014）。

该设备的存储器接口利用存储在存储单元 321（参见图 4）中的初始值 IV_keys，在应用与介质 2 相互验证时生成的会话密钥 Kses 的 CBC 模式下，解密从介质 2 接收的 K′（i）（S1010 到 S1013 和 S1015）。这个解密处理是利用与前面参照图 33 所述的解密处理相同的结构的处理。

借助于上述处理，该设备可以解密加密的内容密钥 Kc 和内容完整性检验值生成密钥 Kicv_cont，从而获得每一个的密钥。

返回到图 35，描述加密文件的读出处理的其余部分。一旦结束作为上述密钥解密处理步骤的步骤 S710，流程转到步骤 S711。在步骤 S711 中，设备的存储器接口在内部把标题设置成“读出标题”，把标题设置成功标志设置成 1（成功），和把忙标志设置成 0（就绪）（S714）。在读出内容时，执行基于设置标题的信息的处理。

另一方面，在步骤 S715 中，控制单元方把状态读出命令发送到存储器接口，并且，在忙标志是 0（就绪）（S716）和标题设置成功标志是 1（成功）（S717）的条件下，转到下一步处理（图 36）。

在图 36 中，在步骤 S721 中，控制单元从文件分配表中获取作为读出对象的内容文件的扇区地址（S（1）到 S（k）），并且，它把扇区 S（i）读出命令依次发送到存储器接口。

一旦接收到扇区 S（i）读出命令（S724），存储器接口就把忙标志设置成 1（忙）（S725），并且，在标题成功标志是 1（成功）（S726）的条件下，移动到下一步骤。在标题成功标志不是 1（失败）的情况下，流程转到步骤 S738，把读出成功标志设置成 0（失败），然后，结束处理。

在标题成功标志是 1（成功）的情况下，判断接收的扇区 S（i）是内部存储器还是外部存储器（S727），并且，在是内部存储器的情况下，判断介质 1 或介质 2 的设置标志是否是 1（指示介质被设置成有效的）（S728），和在设置标志是 1 的情况下，进一步参考块许可表（BPT），判断 BPT 是否把这个作为读出对象的扇区 S（i）设置成允许读出的块（S729）。在存在设置在 BPT 中的读出许可块的情况下，从外部存储器中读出在这个扇区上的数据（S730）。

现在，如果要读出的数据是不受 BPT 管理的内部存储器中的数据，那么，跳过步骤 S728 和 S729。如果在步骤 S728 和 S729 中作出的判断是“否”，即，如果存储这个扇区 S（i）的介质的设置标志不是 1，或者，如果在 BPT 中对于扇区 S（i）没有设置成读出许可，那么，流程转到步骤 S738，把读出成功标志设置成 0，表示读出错误。

如果在步骤 S726 到 S729 的判断块中判断目标扇区 S（i）的读出是可执行的，那么，从存储器中读出这个扇区，并且执行基于与扇区相对应地设置的冗余部分中的纠错码的纠错处理（S731），确认纠错是否已经取得成功（S732）。接着，参考标题（参见图 7）的 ICV 标志，对要读出的扇区是否是通过完整性检验值（ICV）进行处理的对象作出判断。如前面参照图 31 所述，每个扇区存储了用于窜改检验的、在它的冗余部分中的 ICV，因此，可以进行按扇区递增的窜改检验。

在这是通过 ICV 进行窜改检验的对象的情况下，在步骤 734 中，把在步骤 S710 中通过解密处理获得的内容完整性检验值生成密钥 Kicv_cont 和初

的情况下，应用两个内容密钥 Kc（s）和 Kc（s+1mod32）执行每个扇区的加密内容的解密处理（S1109）。

扇区数据的解密处理的不同处理形式显示在图 40 中。在图 40 中，步骤 S1201 到 S1208 与图 39 中的步骤 S1101 到 S1108 相同。步骤 S1209 到 S1211 与图 39 中的那些步骤不同。

在步骤 1205 中，在判断加密算法是三重 DES 的情况下，在步骤 1209 中判断扇区号（s），在 s 是奇数的情况下，执行 s = s-1 的更新处理（S1210），和应用两个内容密钥 Kc（s）和 Kc（s+1）执行每个扇区的加密内容的解密处理（S1211）。

因此，再现处理伴随着通过参照图 35 到图 40 所述的过程对已经加密和存储的数据执行的解密处理。

[数据加密写入处理]

接着，利用从图 41 开始的流程图描述加密写入处理过程的细节。请注意，如上所述，存在着对每个扇区利用不同密钥进行加密的数据加密形式，和利用单个加密密钥加密所有内容的形式。这些形式被设置在标题信息中。在图 41 所示的流程图中，左边是设备的控制单元的处理，右边是在设备的存储器接口上的处理。

首先，控制单元向存储器接口发送与作为读出对象的存储内容相对应的标题生成命令和用作标题信息的参数（S1301）。

一旦接收到标题生成命令（S1302），存储器接口就把忙标志设置成 1（忙）（S1303），并且判断接收的参数是否在容许值之内（S1304）。存储器接口含有可事先设置在标题中的参数范围，因此，可以与接收的参数进行比较，在接收参数超过可设置范围的情况下，在步骤 S1310 中，把标题生成成功标志设置成 0（失败），然后，结束处理。在接收参数在容许值之内的情况下，把标题的有效撤消表版本设置成 0（S1305），以便不参考撤消表就能够进行数据处理。把有效撤消表版本设置成 0 的理由是，在保证经过利用自身设备进行的存储处理的内容是有效内容的假设下，进行不参考撤消表就能够进行数据处理（再现）的设置。

此外，在写入内容例如是通过通信装置从外部接收的内容的情况下，或者，在把标识符加入接收内容中，把撤消表版本存储在标题中，和可以与设备内的撤消表进行核对的情况下，可以按照与前面参照图 35 描述的最后解

始值 IVcont 用于输入作为窜改检验对象（扇区数据）的数据和执行参照图 14 所述的 ICV 生成处理，获取 ICV′，将其与存储在扇区的冗余部分中的 ICV 进行核对，并且在它们相匹配的情况下，作出无窜改判断。

在通过 ICV 检验作出无窜改判断的情况下，流程转到步骤 S736，进行根据标题信息解密数据的处理（S736），并且，把读出成功标志设置成 1（成功），和把解密数据存储在缓冲器中。

此外，在步骤 S740 到 S746 中，控制单元读出存储器接口的状态，并且，在忙标志是 0 的状态下，和在读出成功标志是 1 的条件下，从缓冲器中提取读出数据和保存它，然后，依次递增地址，重复执行从缓冲器中依次提取数据和保存它的处理，和在保存了作为读出对象的所有扇区之后，该文件由已经读出的所有扇区构成，然后，结束处理。

下面参照图 39 描述图 36 的步骤 S736 中数据解密处理的细节。这个解密处理是在设备的存储器接口的加密处理单元 320（参见图 4）上执行的。

首先，把用于存储作为解密对象的数据的扇区位置设为 s（其中，$0 \leq s \leq 31$（在扇区数是 32 的情况下））（S1101）。接着，检验该扇区是否是加密对象（S1102）。这个检验是根据保密标题（参见图 7）中的加密标志判断的。在不是加密对象的情况下，不执行解密处理，然后，结束处理。在是加密对象的情况下，检验加密格式类型（S1103）。这个检验包括检验在保密标题内加密格式类型的设置，和判断对于如图 8 所述的所有内容，加密格式是否是 1，或对于每个扇区，加密处理是否使用了不同的密钥。

在加密格式类型的设置值是 0 的情况下，这是其中对于所有内容，加密格式是 1 的情况。在这种情况中，在步骤 S1104 中判断加密算法。对于加密算法，设置了单重 DES 或三重 DES（参见图 28），在判断这是单重 DES 的情况下，利用一个内容密钥 Kc（0）执行加密内容的解密处理（S1106）。在判断这是三重 DES 的情况下，应用两个内容密钥 Kc（0）和 Kc（1）执行加密内容的解密处理（S1107）。

另一方面，在步骤 S1103 中，在加密格式类型的设置值是 1 的情况下，这是其中对于每个扇区，加密处理使用不同密钥的情况。在这种情况中，在步骤 S1105 中判断加密算法。对于加密算法，设置了单重 DES 或三重 DES（参见图 28），在判断这是单重 DES 的情况下，应用与每个扇区相对应地设置的内容密钥 Kc（s）执行加密内容的解密处理（S1108）。在判断这是三重 DES

密读出处理中执行的步骤 S707 到 S709 相同的方式进行利用撤消表的标识符核对处理，来代替上述处理。

接着，在步骤 S1306 中，生成和加密内容密钥 Kc 和内容完整性检验值（ICV）生成密钥 Kicv_cont。图 43 说明了步骤 S1306 中内容密钥 Kc 和内容完整性检验值（ICV）生成密钥 Kicv_cont 的生成和解密处理的细节。图 43 所示的处理是在设备的加密处理单元 320（参见图 4）的存储器接口上执行的。下面描述图 43 所示的流程图。

首先，根据，例如，使其成为加密对象的随机数，生成加密内容完整性检验值生成密钥 Kicv_cont，其次，对标题中加密格式类型字段是否被设置成 0 作出判断（S1402）。在加密格式类型字段是 0 的的情况下，这时利用一种与扇区无关的形式加密整个内容的结构，和在加密格式类型字段被设置为 0 的的情况下，这是如前面参照图 27 和其它附图描述的、按扇区递增的方式利用加密密钥的方法。在按扇区递增的方式利用加密密钥的情况下，流程转到步骤 S1403，在步骤 S1403 中，生成为每个扇区设置的内容密钥（Kc（0）到 Kc（31）（在扇区数是 32 的情况下）），使其成为加密对象。

如果在步骤 S1402 中判断加密格式类型字段是 0，那么，在步骤 S1404 中进一步检验标题中的加密算法字段，并且对加密算法字段是 1（三重 DES）还是 0（单重 DES）加以判断。在是单重 DES 的情况下，在步骤 S1405 中生成一个加密内容密钥（Kc（0）），并且将其加入加密对象中，和是三重 DES 的情况下，在步骤 S1406 中生成多个加密内容密钥（Kc（0），Kc（1）），并且将其加入加密对象中。

接着，在步骤 S1407 中，检验标题中内容类型字段的设置，和在设置不是 2 或 3（介质 2 存储内容）的情况下，在步骤 S1408 中，把存储在存储单元 321（参见图 4）中的分配密钥 Kdist 用于加密数据，即，内容完整性检验值生成密钥 Kicv_cont 和一个或多个内容密钥。

在设置是 2 或 3（介质 2 存储内容）的情况下，在步骤 S1409 中，利用介质 2 的存储密钥 Ksto（CBC 模式）加密数据，即，内容完整性检验值生成密钥 Kicv_cont 和一个或多个内容密钥。这个加密处理的细节如参照图 32、图 33 和图 34 所述。

下面参照图 44 所示的流程图描述通过介质 2 的存储密钥对内容完整性检验值生成密钥 Kicv_cont 和一个或多个内容密钥的加密处理。在图 44 所

示的流程图中，左边表示设备的存储器接口的处理，右边表示介质 2（参见图 2）的控制器上的处理。

首先，设备方上的存储器接口把要加密的数据设置成 K（0）到 K（n-1）（内容完整性检验值生成密钥 Kicv_cont 和一个或多个内容密钥）（S1501），应用在与介质 2 相互验证时生成的会话密钥，利用存储在存储单元 321 中的初始值 IV_keys，在 DES-CBC 模式下，执行对要加密的数据 K（0）到 K（n-1）的加密处理，和生成数据 K′（0）到 K′（n-1）（S1502）。这个加密处理是通过与如前所述的图 32 所示的处理结构相同的处理结构执行的。接着，存储器接口把 CBC 加密初始化命令发送到介质 2 控制器（S1504）。介质 2 控制器把存储在介质 2 中的初始值 IV_keys 设置到寄存器中（S1506）。随后，存储器接口依次发送密钥（S1505）。

介质 2 控制器接收数据 K′（i）（S507），利用与设备相互验证时生成的会话密钥，在 CBC 模式下对接收数据 K′（i）进行解密处理（S1508），和获取解密的密钥数据（例如，与多个扇区相对应的内容密钥）（S1509）。接着，介质 2 控制器利用介质 2 的存储密钥 Ksto，在 CBC 模式下，对解密的密钥数据串进行加密处理，生成数据串 K"（i），和把结果发送到设备（S1510）。步骤 S1507 到 S1510 的处理是根据前面参照图 34 所述的、在 DES-CBC 模式下的处理进行的。

设备的存储器接口依次接收 K"（i），并且，在确认已经接收到所有数据之后，把 CBC 结束命令发送到介质 2 控制器（S1511 到 S1514）。一旦接收到 CBC 结束命令，介质 2 控制器就清除寄存器（S1515）。

设备的存储器接口把从介质 2 接收的 K"（0）到 K"（n-1）取作用于标题存储的加密密钥数据。由于上述处理，设备可以获得要存储在标题中的加密内容密钥 Kc 和内容完整性检验值生成密钥 Kicv_cont。

返回到图 41，继续描述文件加密写入处理。一旦在步骤 S1306 结束时生成和加密上述标题存储密钥，存储器接口就根据生成的标题数据生成完整性检验值 ICV（S1307）。利用存储在存储单元 321（参见图 4）中的初始值 IVsh 和保密标题完整性检验值生成密钥 Kicv_sh，根据前面参照图 14 所述的 ICV 生成结构，生成作为保密标题的检验值的 ICV_sh。接着，在步骤 S1308 中，在内部把生成的标题保存成“写入标题”，并且，在步骤 S1309 中把标题生成成功标志设置成 1（成功）和在步骤 S1311 中把忙标志设置成 0（就绪），

然后，结束处理。

另一方面，控制单元方在步骤 S1312 中把状态读出命令发送到存储器接口，在忙标志是 0（就绪）（S1313）和标题生成成功标志是 1（成功）（S1314）的条件下，从缓冲器当中读取标题，和将其保存在介质中作为一般文件（S1350），之后，流程转到下一步处理（图 42）。

在图 42 的步骤 S1321 中，控制单元把要写入的内容文件划分成若干个扇区。分成的数据用 D（1）到 D（k）表示。 控制单元为数据 D（i）设置写扇区 S（i），接着，把有关扇区 S（i）的加密写入命令和数据 D（i）发送到存储器接口（S1322 到 S1324）。一旦接收到扇区 S（i）加密写入命令（S1325），存储器接口就把忙标志设置成 1（忙）（S1326），并且，在标题生成成功标志是 1（成功）（S1327）的条件下，转动到下一步骤。

接着，存储器接口判断接收的扇区 S（i）是内部存储器还是外部存储器（S1328），并且，在是外部存储器的情况下，判断介质 1 或介质 2 的设置标志是否是 1（指示介质被设置成有效的）（S1329），和在设置标志是 1 的情况下，进一步参考块许可表（BPT），判断 BPT 是否把这个作为写对象的扇区 S（i）设置成写入许可块（S1330）。如果在 BPT 中存在像写入许可块那样的设置，那么，生成与扇区相对应地设置的纠错码（S1331）。

接着，根据标题信息（ICV 标志），判断写入扇区是否是 ICV 设置扇区（S1332），和在是 ICV 的对象的情况下，根据内容 ICV 生成密钥 Kicv_cont 生成扇区数据的 ICV（S1333）。

接着，存储器接口根据标题信息，进行数据的加密处理（S1334）。下面参照图 45 描述步骤 S1334 中这个数据加密处理的细节。这个加密处理是在设备的存储器接口的加密处理单元 320（参见图 4）上执行的。

首先，把用于存储作为加密对象的数据的扇区位置设为 s（其中，$0 \leq s \leq 31$）（在扇区数是 32 的情况下）（S1601）。接着，检验该扇区是否是加密对象（S1602）。这个检验是根据保密标题（参见图 7）中的加密标志判断的。在不是加密对象的情况下，不执行加密处理，然后，结束处理。在是加密对象的情况下，检验加密格式类型（S1603）。这个检验包括检验在保密标题内加密格式类型的设置，和判断对于如图 8 所述的所有内容，加密格式是否是 1，或对于每个扇区，加密处理是否使用了不同的密钥。

在加密格式类型的设置值是 0 的情况下，这是对于所有内容，加密格式

是1的情况。在这种情况中，在步骤S1604中判断加密算法。对于加密算法，设置了单重DES或三重DES（参见图28），在判断是单重DES的情况下，利用一个内容密钥Kc（0）执行加密内容的加密处理（S1606）。在判断是三重DES的情况下，应用两个内容密钥Kc（0）和Kc（1））执行加密内容的加密处理（S1607）。

另一方面，在步骤S1603中，在加密格式类型的设置值是1的情况下，这是对于每个扇区，加密处理使用不同密钥的情况。在这种情况中，在步骤S1605中判断加密算法。对于加密算法，设置了单重DES或三重DES（参见图28），在判断是单重DES的情况下，应用与每个扇区相对应地设置的内容密钥Kc（s）执行加密内容的加密处理（S1608）。在判断是三重DES的情况下，应用两个内容密钥Kc（s）和Kc（s+1mod32）执行每个扇区的加密内容的加密处理（S1609）。

扇区数据的加密处理的不同处理形式显示在图46中。在图46中，步骤S1701到S1708与图45中的步骤S1601到S1608相同。步骤S1709到S1711与图45中的那些步骤不同。

在步骤1705中，在判断加密算法是三重DES的情况下，在步骤1209中判断扇区号（s），在s是奇数的情况下，执行s=s-1的更新处理（S1710），和应用两个内容密钥Kc（s）和Kc（s+1）执行每个扇区的加密内容的加密处理（S1711）。

返回到图42，继续描述文件加密写入处理流程。一旦通过上述处理结束数据部分的加密处理步骤（S1334），就为数据部分生成纠错码（S1335），和把加密的数据D（i）和含有与扇区相对应的完整性检验值ICV和纠错码的冗余部分写入介质中（S1336），把写入成功标志设置成1（成功）（S1337），和把忙标志设置成0（就绪）（S1339）。

现在，如果要写入的数据是写入不受BPT管理的外部存储器中的数据，那么，跳过步骤S1329和S1330。如果在步骤S1329和S1330中作出的判断是“否”，即，如果介质的设置标志不是1，或者，如果在BPT中对于扇区S（i）没有设置成写入许可，那么，流程转到步骤S1338，把写入成功标志设置成0，表示写入错误。

此外，在步骤S1341到S1345中，控制单元读出存储器接口的状态，并且，在忙标志是0的状态下，和在写入成功标志是1的条件下，依次递增地

址，和把写入数据依次发送到存储器接口。和在结束所有处理之后，执行文件分配表的更新处理（S1346），把更新的文件分配表与更新命令一道发送到存储器接口（S1347），和存储器接口根据命令执行写入文件分配表的处理（S1340）。

数据的加密和存储到介质的处理是通过上面参照图 41 到图 46 所述的处理进行的。

[更新撤消表]

接着，对更新作为未授权介质和内容的失效信息的撤消表的处理加以描述。如上所述，根据本发明的撤消表由多种类型（例如，介质和内容）的标识符（ID）构成。通过在作为内容和介质的失效信息的撤消表中提供多种类型的 ID，并且可以作为不同的操作进行它们的核对处理，可以用单个撤消表撤消多个内容和介质。在插入介质或读出内容时，通过在所使用的介质或所使用的内容的标识符（ID）与列在存储器接口单元上的撤消表中的 ID 之间进行核对，可以禁止未授权介质的使用和未授权内容的读出。

如上所述，在撤消表中设置了撤消表版本，因此，在加入未授权介质或内容的新失效信息等的情况下，更新撤消表。

图 47 显示了撤消表更新处理的流程图。在图 47 中，左边是设备的控制单元，右边是设备的存储器接口。

首先，一旦从通信单元 201（参见图 2）接收到更新撤消表（S1801），控制单元就把更新撤消表检验命令和接收的更新撤消表发送到存储器接口（S1802）。

一旦从控制单元接收到更新撤消表检验命令和更新撤消表（S1803），存储器接口就把忙标志设置成 1（忙）（S1804），和生成用于撤消表的完整性检验值（ICV）生成密钥 Kicv_r1（S1805）。

用于撤消表窜改检验的完整性检验值（ICV）生成密钥 Kicv_r1 是根据用于生成事先存储在设备内的撤消表的 ICV 密钥的主密钥 MKicv_r1、供生成撤消表的 ICV 密钥时使用的初始值 IVicv_r1、和包含在撤消表的属性信息中的撤消表版本生成的。具体地说，完整性检验值（ICV）生成密钥是根据完整性检验值（ICV）生成密钥 Kicv_r1 = DES（E，MKicv_r1，Version^IVicv_r1）生成的。这个方程的含义是根据版本与初始值（IVicv_r1）的异或运算结果，利用主密钥 MKicv_r1，在 DES 模式下进行

加密处理。

接着，存储器接口利用完整性检验值（ICV）生成密钥 Kicv-r1 生成撤消表的 ICV′（S1806），和执行与事先存储在撤消表中的正确 ICV 的核对处理 ICV′ = ICV？（S1807）。ICV′的生成处理是通过根据参照上面图 14 所述的 DES 模式，应用生成的完整性检验值（ICV）生成密钥 Kicv-bpt 和利用初始值 IVicv-bpt 的处理进行的。

在 ICV′ = ICV 成立的情况下（在 S1807 中的“是”），判断存储撤消表是有效的，即没有被窜改，流程转到步骤 S1808，将当前设置的撤消表的版本（i）与更新撤消表版本（j）相比较（S1809），和在更新撤消表版本较新的情况下，把更新撤消表有效标志设置成 1（S1810），把忙标志设置成 0（S1811），然后，结束处理。

另一方面，控制单元方把状态读出命令发送到存储器接口（S1812），确认忙标志是否是 0（S1813），并且，在更新撤消表有效标志是 1 的情况下（S1814），把更新撤消表保存在内部存储器中作为一般文件（S1815）。在处理内容或安装介质时，如果需要检验，就读出存储在内部存储器中的撤消表。

至此，通过结合特定的实施例已经对本发明作了描述。但是，对于本领域的普通技术人员来说，不言而喻，可以对实施例作各种各样的修改和替换而不偏离本发明的精神或范围。换言之，本发明是以举例的方式得以公开的，不应该把实施例理解为限制性的。本发明的范围由所附的权利要求书唯一地确定。

工业可应用性

如上所述，根据本发明的数据再现设备和数据记录设备、数据再现方法和数据记录方法、和表格更新方法，把版本信息设置在撤消表中，因此，在读出内容时，将设备当前保存的撤消表的版本与标题中的有效撤消表相比较，在当前保存的撤消表的版本较旧的情况下，取消内容的读出。这样，如果不更新撤消表，就不能读出内容，因此，可以撤消利用旧撤消表对内容的未授权使用。

并且，根据本发明的数据再现设备和数据记录设备、数据再现方法和数据记录方法、和表格更新方法，在撤消表的更新处理过程中，还将，例如，从通信路径接收的更新撤消表的版本与当前撤消表的版本信息相比较，只有在判断更新撤消表是较新撤消表的情况下，才允许撤消表得到更新，因此，

可以防止利用旧撤消表非法取代撤消表的处理。

并且，根据本发明的数据再现设备和数据记录设备、数据再现方法和数据记录方法、和程序提供介质，把撤消表建立到存储器接口上，在建立之后，当安装介质时或当再现内容时，可以在存储器接口上不断使用它，这样就避免了诸如在使用内容时，从内部存储器重复读出之类的处理，从而，可以有效地进行处理。

并且，根据本发明的数据再现设备和数据记录设备、数据再现方法和数据记录方法、和程序提供介质，把撤消表建立到存储器接口上，并且，在建立之后，当安装介质时或当再现内容时，可以在存储器接口上不断使用它，并且，提供了作为撤消对象的多种类型的 ID，即介质 ID 和内容 ID，使利用单个撤消表的核对处理可在每一个的设备方上执行，因此，可以利用一次性设置在存储器接口上的撤消表撤消多种内容和介质，从而，有效地执行在插入介质或读出内容时，在存储器接口单元上进行的撤消表参考处理，和可以有效地禁止未授权介质的使用和未授权内容的读出。

并且，根据本发明的数据再现设备和数据记录设备、数据再现方法和数据记录方法、和程序提供介质，把属于不同类别的、介质和内容两者的标识符存储在一个撤消表中，因此，可以根据单个撤消表进行未授权介质和未授权内容的撤消，从而，减少了保存在设备方上的撤消表，和减轻了当安装介质和使用内容时在设备方上的处理。

并且，根据本发明的数据再现设备和数据记录设备、数据再现方法和数据记录方法、和程序提供介质，把作为撤消对象的多种类型的 ID，即，介质 ID 和内容 ID 提供到作为内容和介质的失效信息的撤消表中，并且，在每一个的设备方上可以作为不同的操作进行它的核对处理，例如，在安装介质时与介质标识符核对，和在再现内容时与内容标识符核对，因此，可以利用单个撤消表撤消多种内容和介质，从而，有效地执行在插入介质或读出内容时，在存储器接口单元上进行的撤消表参考处理，和可以有效地禁止未授权介质的使用和未授权内容的读出。

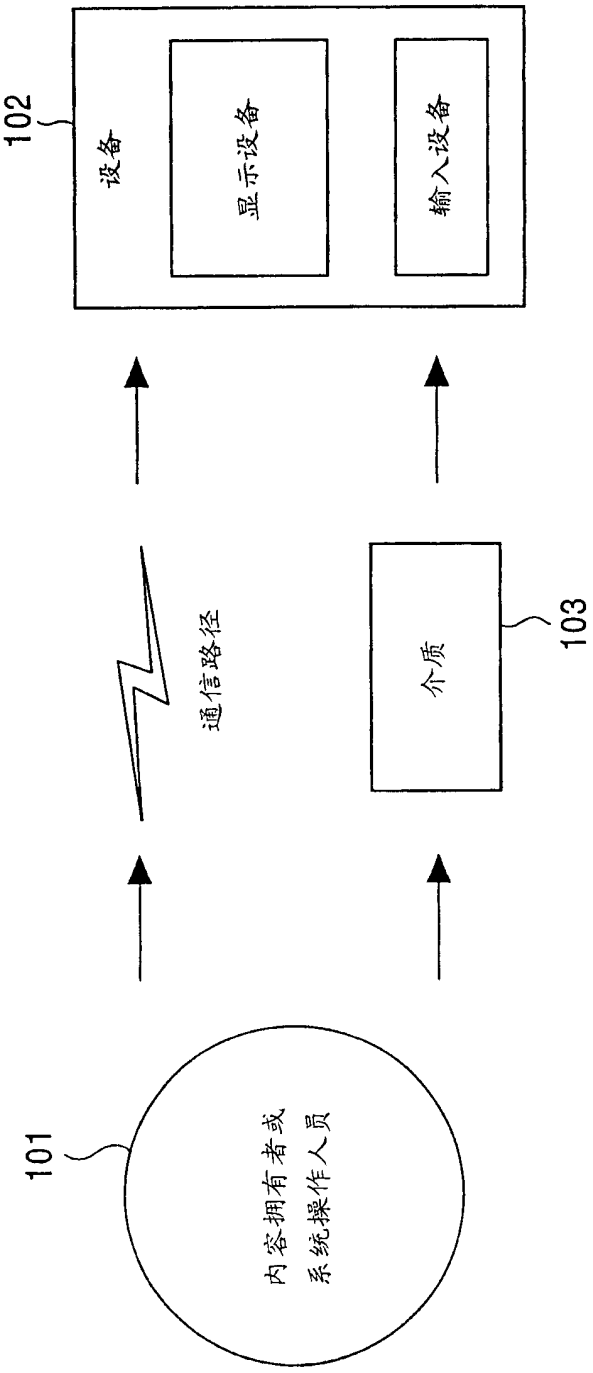


图 1

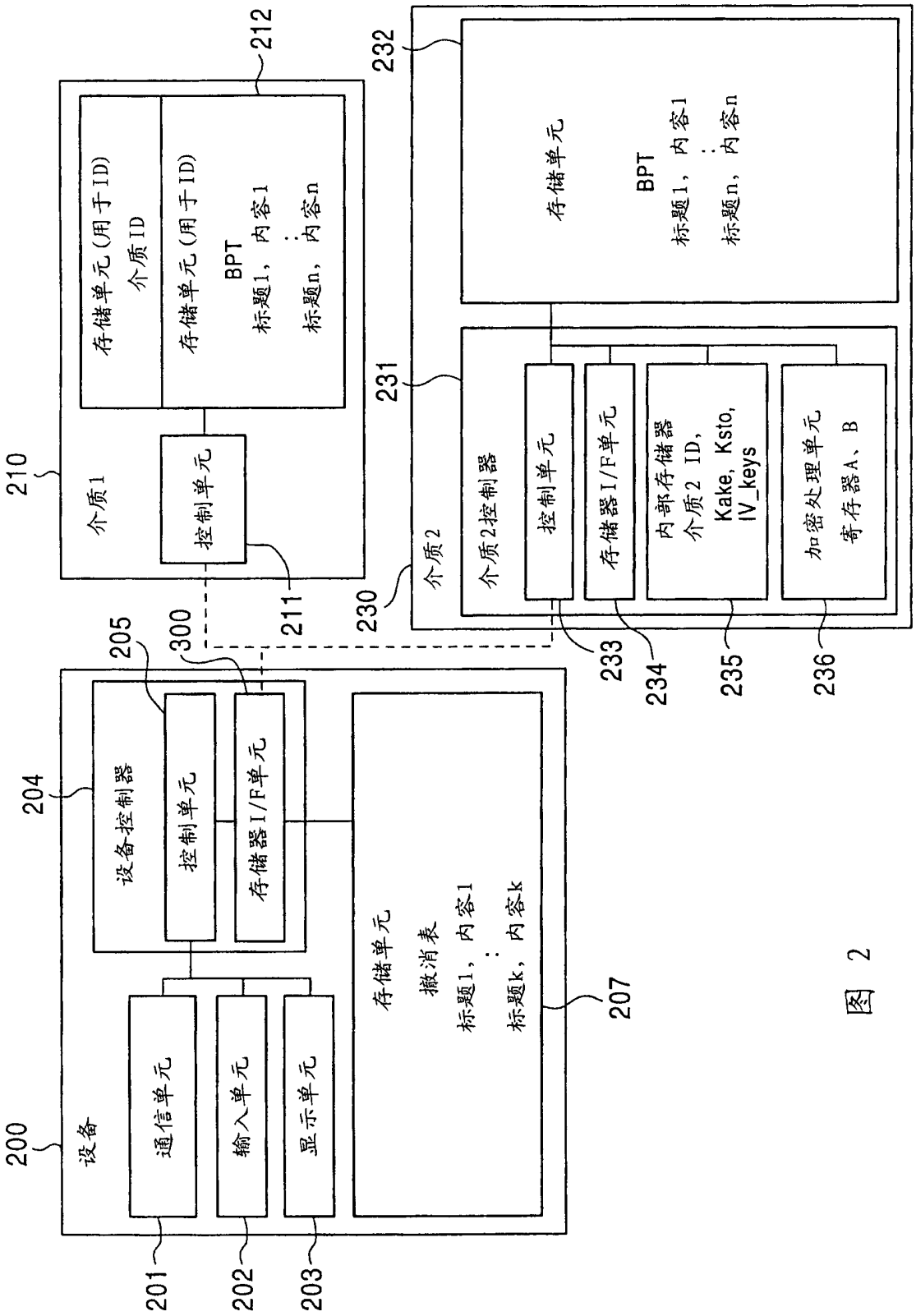

200
设备
通信单元
输入单元
显示单元
201
202
203
204
设备控制器
控制单元
存储器I/F单元
205
300
存储单元
撤消表
标题1，内容1
：
标题k，内容k
207
210
介质1
存储单元(用于ID)
介质ID
存储单元(用于ID)
BPT
标题1，内容1
：
标题n，内容n
212
控制单元
211
230
介质2
231
介质2控制器
控制单元
存储器I/F单元
内部存储器
介质2 ID，
Kake，Ksto，
IV_keys
加密处理单元
寄存器A、B
232
存储单元
BPT
标题1，内容1
：
标题n，内容n
233
234
235
236

图 2

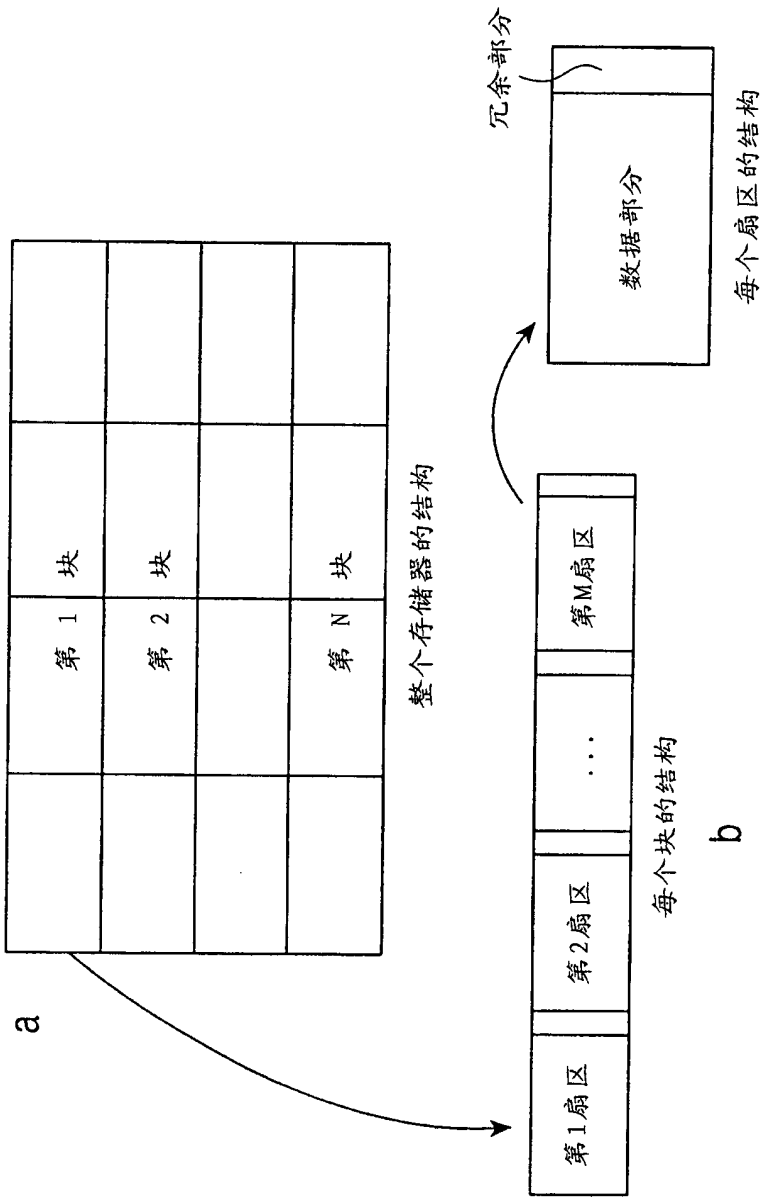

a
第 1 块
第 2 块
第 N 块
整个存储器的结构
b
第1扇区
第2扇区
...
第M扇区
每个块的结构
c
冗余部分
数据部分
每个扇区的结构

图 3

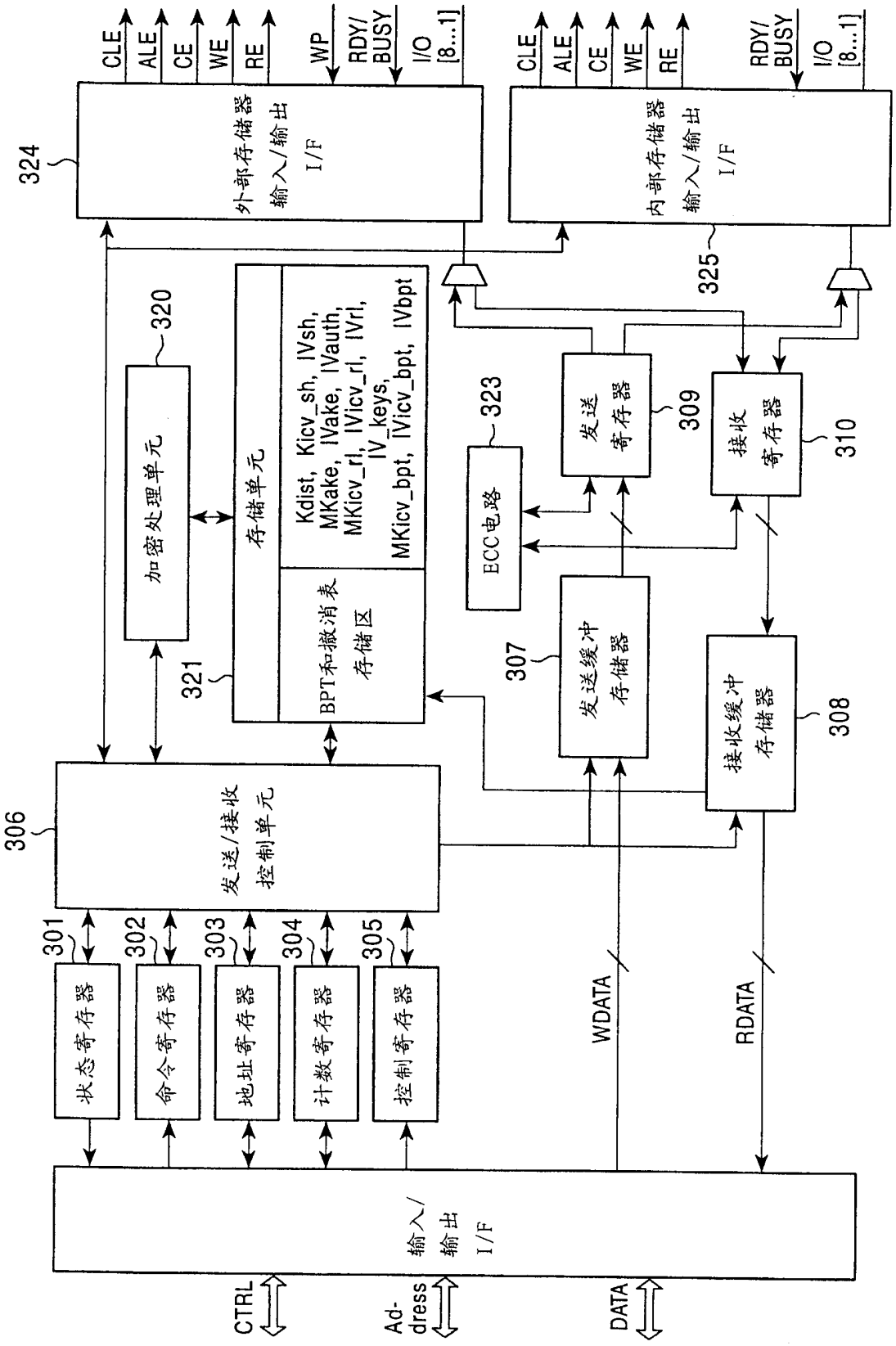

CLE
ALE
CE
WE
RE
WP
RDY/BUSY
I/O [8...1]
外部存储器输入/输出 I/F
324
内部存储器输入/输出 I/F
325
加密处理单元
320
存储单元
Kdist, Kicv_sh, IVsh, MKake, IVake, IVauth, MKicv_rl, IVicv_rl, IVrl, IV_keys, MKicv_bpt, IVicv_bpt, IVbpt
BPT和撤消表存储区
321
ECC电路
323
发送寄存器
309
接收寄存器
310
发送缓冲存储器
307
接收缓冲存储器
308
发送/接收控制单元
306
状态寄存器
301
命令寄存器
302
地址寄存器
303
计数寄存器
304
控制寄存器
305
WDATA
RDATA
输入/输出 I/F
CTRL
Ad-dress
DATA

图 4

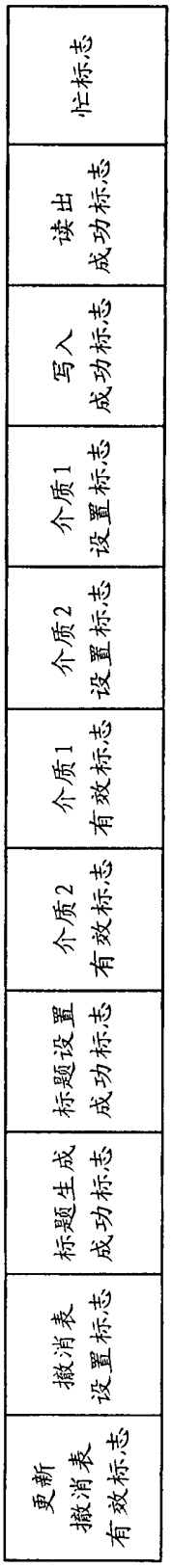
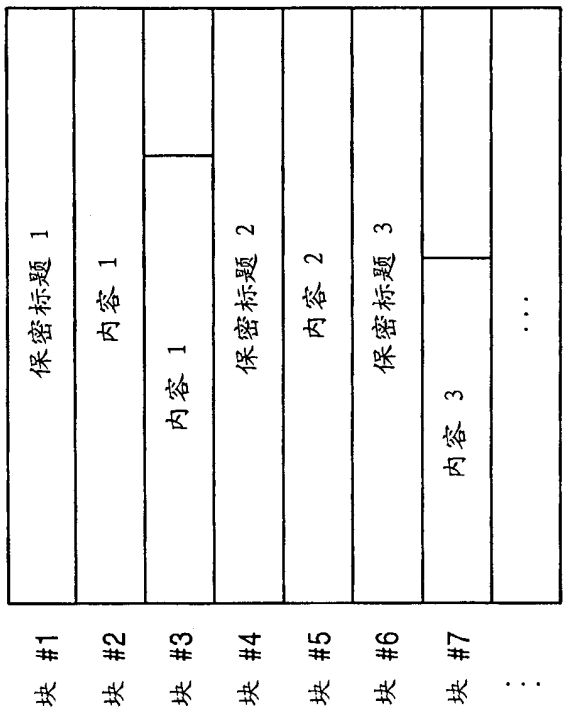

位 10
位 9
位 8
位 7
位 6
位 5
位 4
位 3
位 2
位 1
位 0
更新撤消表有效标志
撤消表设置标志
标题生成成功标志
标题设置成功标志
介质2有效标志
介质1有效标志
介质2设置标志
介质1设置标志
写入成功标志
读出成功标志
忙标志

图 5



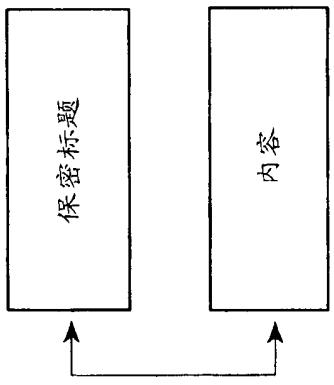


图 6


格式版本
内容ID
内容类型
数据类型
加密算法
加密模式
加密格式类型
加密标志
ICV标志
加密内容密钥 (Kc0)
...
加密内容密钥 (Kc31)
加密ICV生成密钥 (Kicv)
有效撤消表版本
加密标题的ICV

图 7

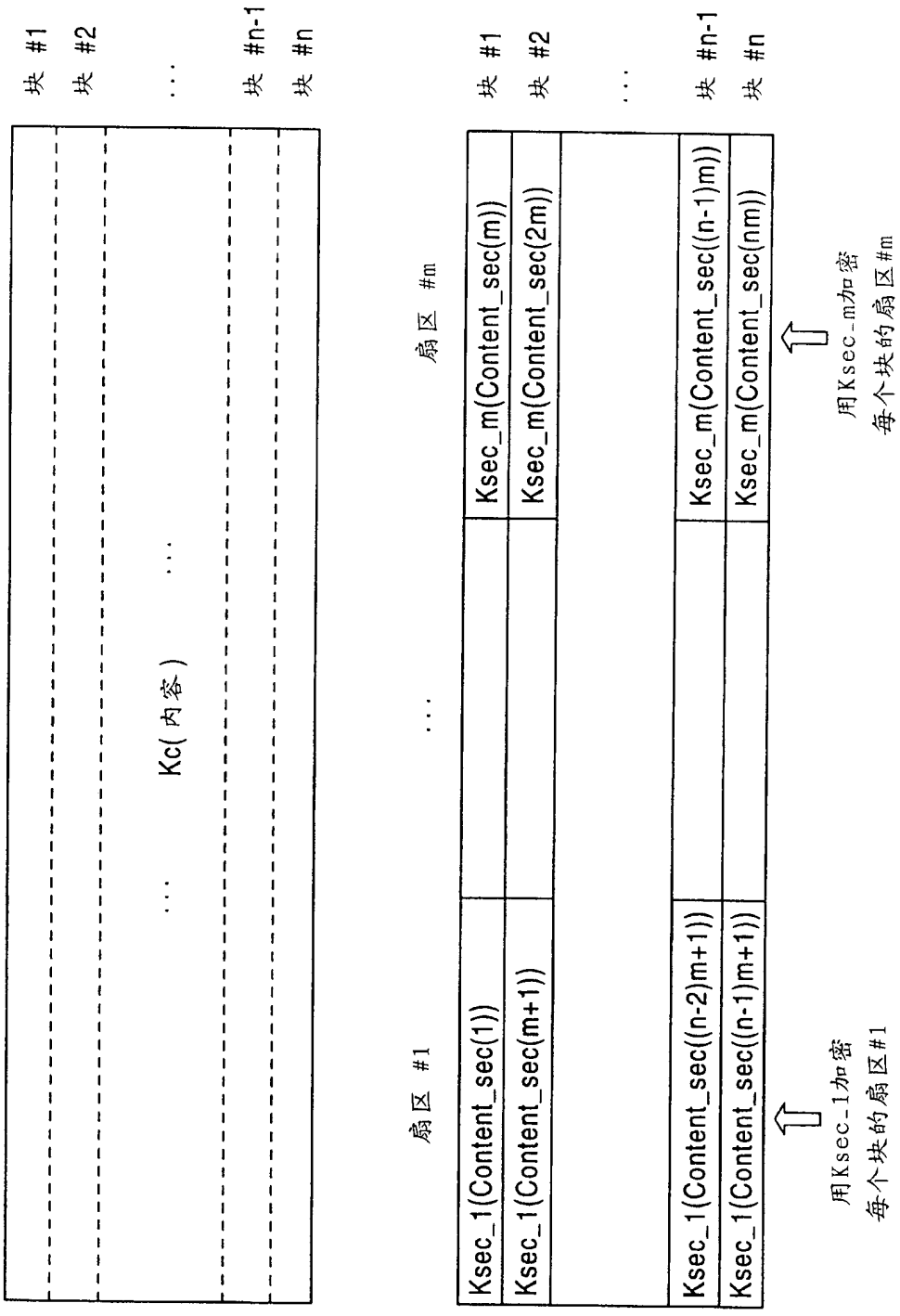

块 #1
块 #2
...
块 #n-1
块 #n
Kc(内容)
...
扇区 #1
扇区 #m
Ksec_1(Content_sec(1))
Ksec_1(Content_sec(m+1))
Ksec_1(Content_sec((n-2)m+1))
Ksec_1(Content_sec((n-1)m+1))
Ksec_m(Content_sec(m))
Ksec_m(Content_sec(2m))
Ksec_m(Content_sec((n-1)m))
Ksec_m(Content_sec(nm))
用Ksec_1加密
每个块的扇区#1
用Ksec_m加密
每个块的扇区#m

图 8

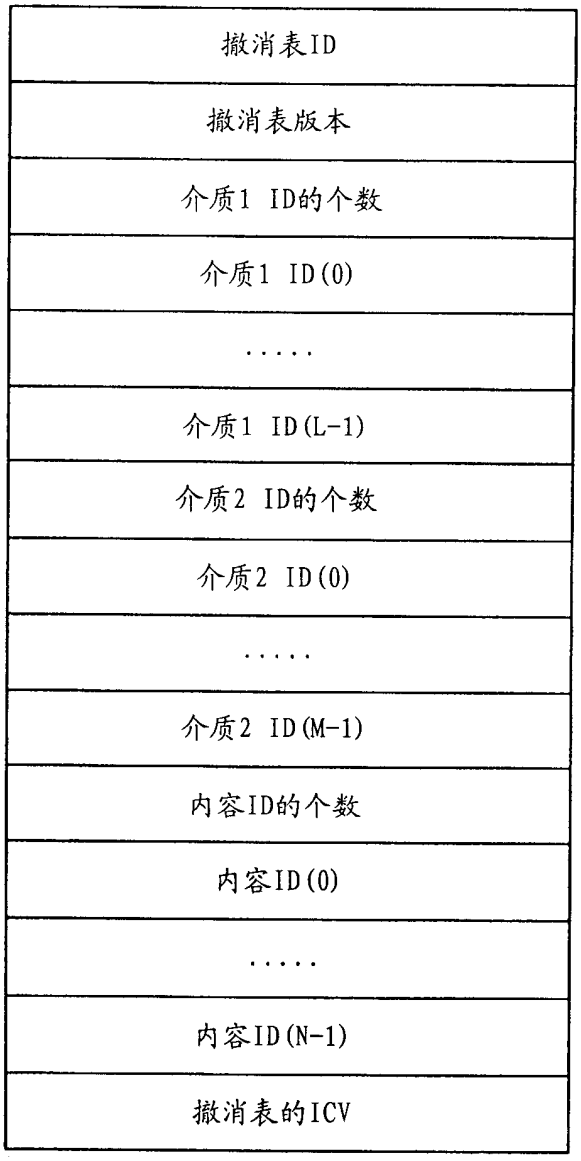

撤消表ID
撤消表版本
介质1 ID的个数
介质1 ID(0)
.....
介质1 ID(L-1)
介质2 ID的个数
介质2 ID(0)
.....
介质2 ID(M-1)
内容ID的个数
内容ID(0)
.....
内容ID(N-1)
撤消表的ICV

图 9

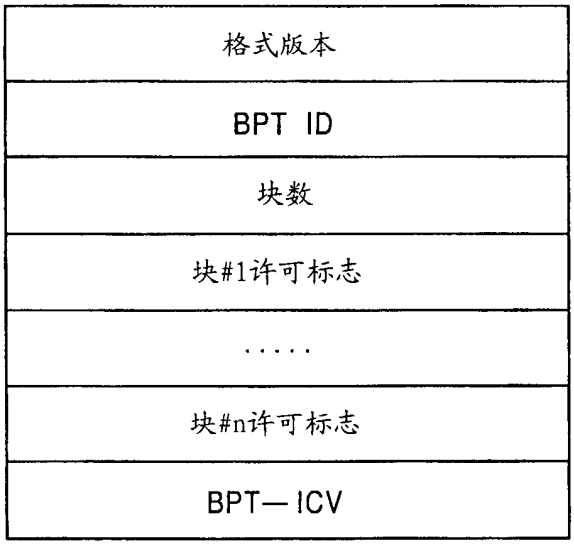


图 10

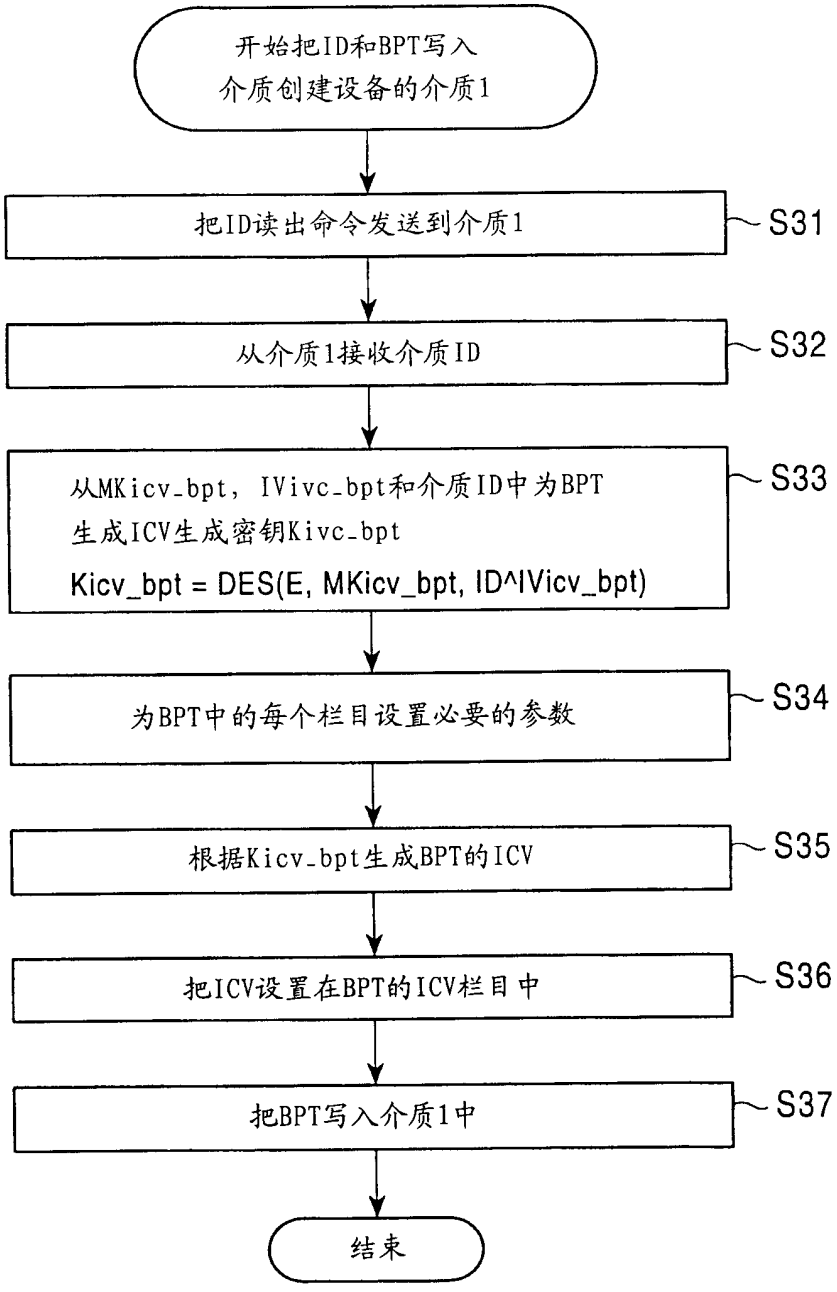

开始把ID和BPT写入
介质创建设备的介质1
把ID读出命令发送到介质1
S31
从介质1接收介质ID
S32
从MKicv_bpt, IVivc_bpt和介质ID中为BPT
生成ICV生成密钥Kivc_bpt
Kicv_bpt = DES(E, MKicv_bpt, ID^IVicv_bpt)
S33
为BPT中的每个栏目设置必要的参数
S34
根据Kicv_bpt生成BPT的ICV
S35
把ICV设置在BPT的ICV栏目中
S36
把BPT写入介质1中
S37
结束

图 11

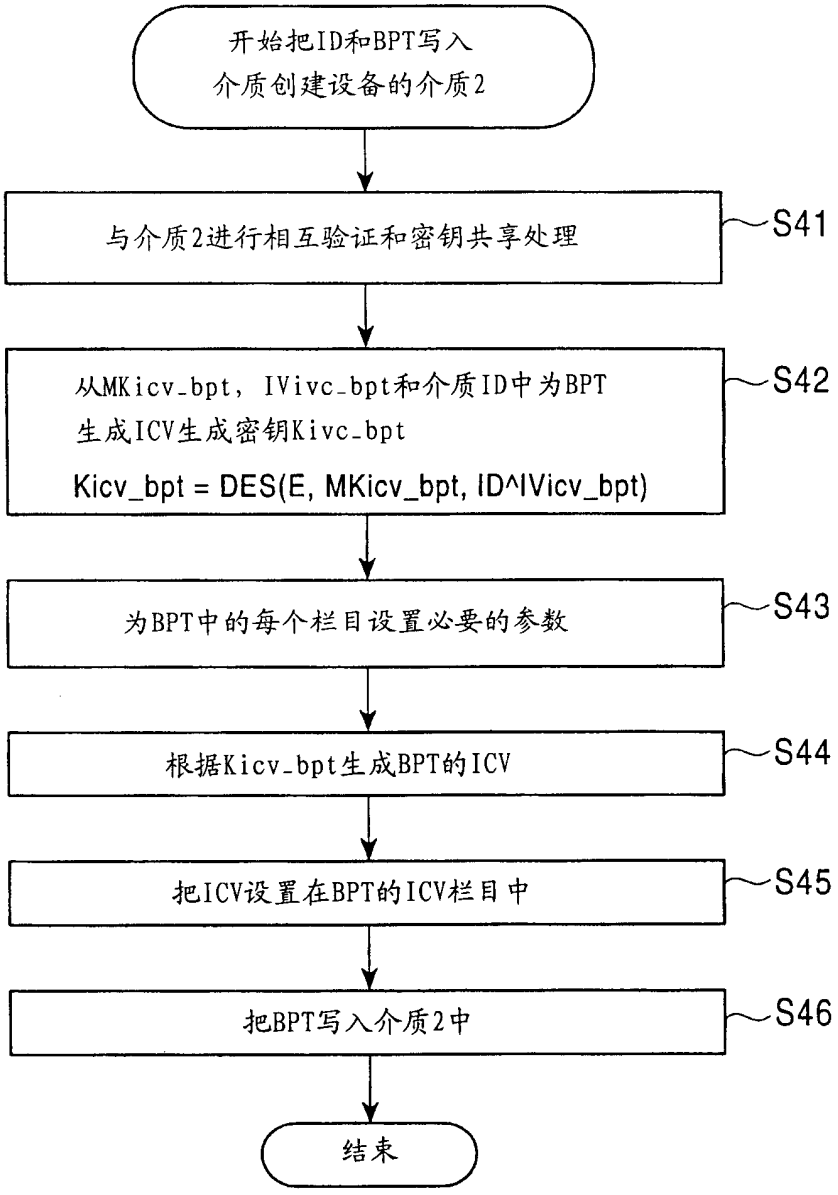

开始把ID和BPT写入
介质创建设备的介质2
与介质2进行相互验证和密钥共享处理
S41
从MKicv_bpt，IVivc_bpt和介质ID中为BPT
生成ICV生成密钥Kivc_bpt
Kicv_bpt = DES(E, MKicv_bpt, ID^IVicv_bpt)
S42
为BPT中的每个栏目设置必要的参数
S43
根据Kicv_bpt生成BPT的ICV
S44
把ICV设置在BPT的ICV栏目中
S45
把BPT写入介质2中
S46
结束

图 12

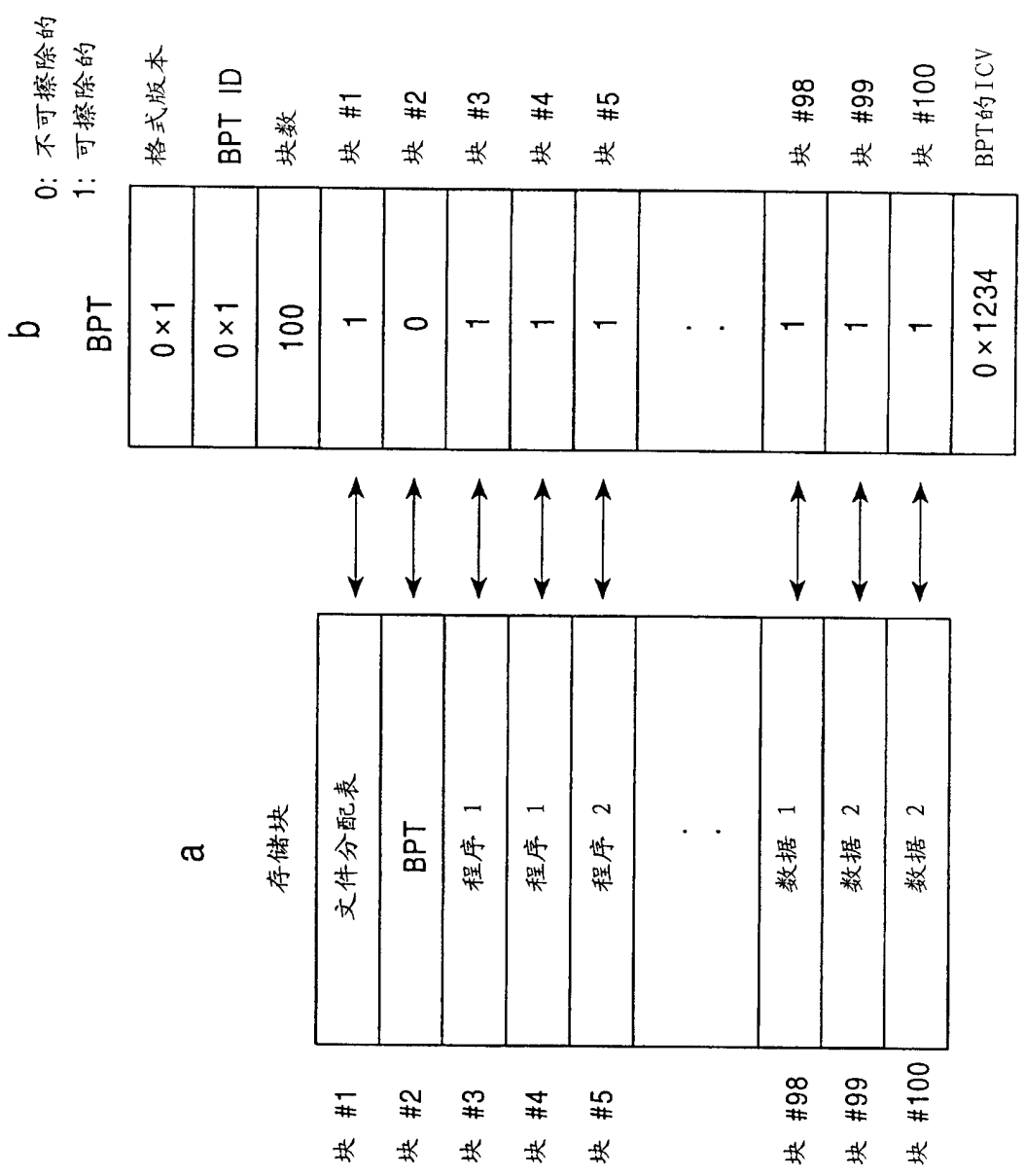

a
存储块
文件分配表
BPT
程序 1
程序 1
程序 2
数据 1
数据 2
块 #1
块 #2
块 #3
块 #4
块 #5
块 #98
块 #99
块 #100
b
BPT
0×1
0×1
100
1
0
1
1
1
1
1
1
0×1234
格式版本
BPT ID
块数
块 #1
块 #2
块 #3
块 #4
块 #5
块 #98
块 #99
块 #100
BPT的ICV
0: 不可擦除的
1: 可擦除的

图 13

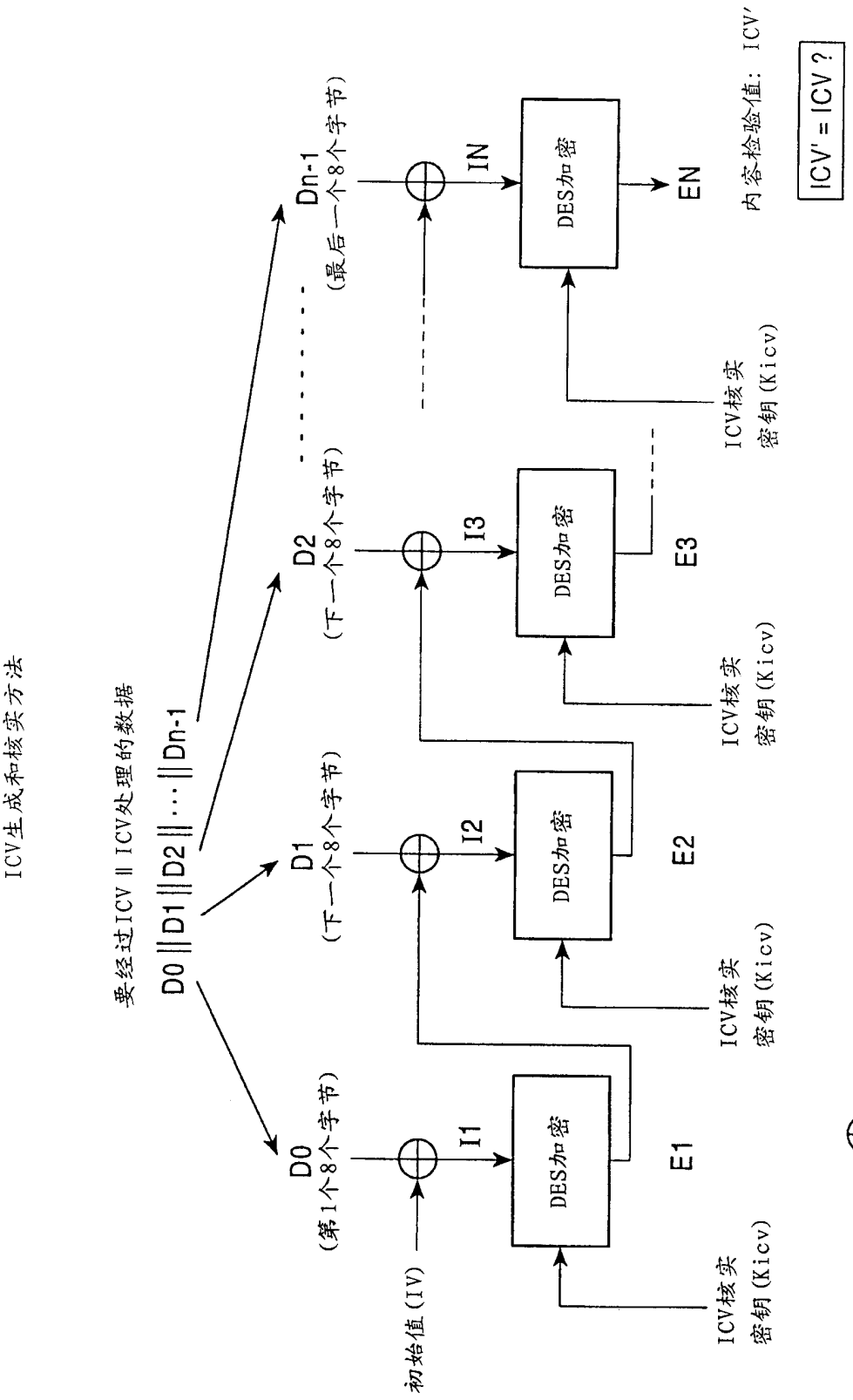

ICV生成和核实方法
要经过ICV ‖ ICV处理的数据
D0 ||D1 ||D2 || ··· ||Dn-1
D0
(第1个8个字节)
D1
(下一个8个字节)
D2
(下一个8个字节)
Dn-1
(最后一个8个字节)
初始值(IV)
I1
I2
I3
IN
DES加密
E1
E2
E3
EN
ICV核实
密钥(Kicv)
内容检验值: ICV′
ICV′ = ICV ?
⊕: 异或处理(按8-字节递增)

图 14

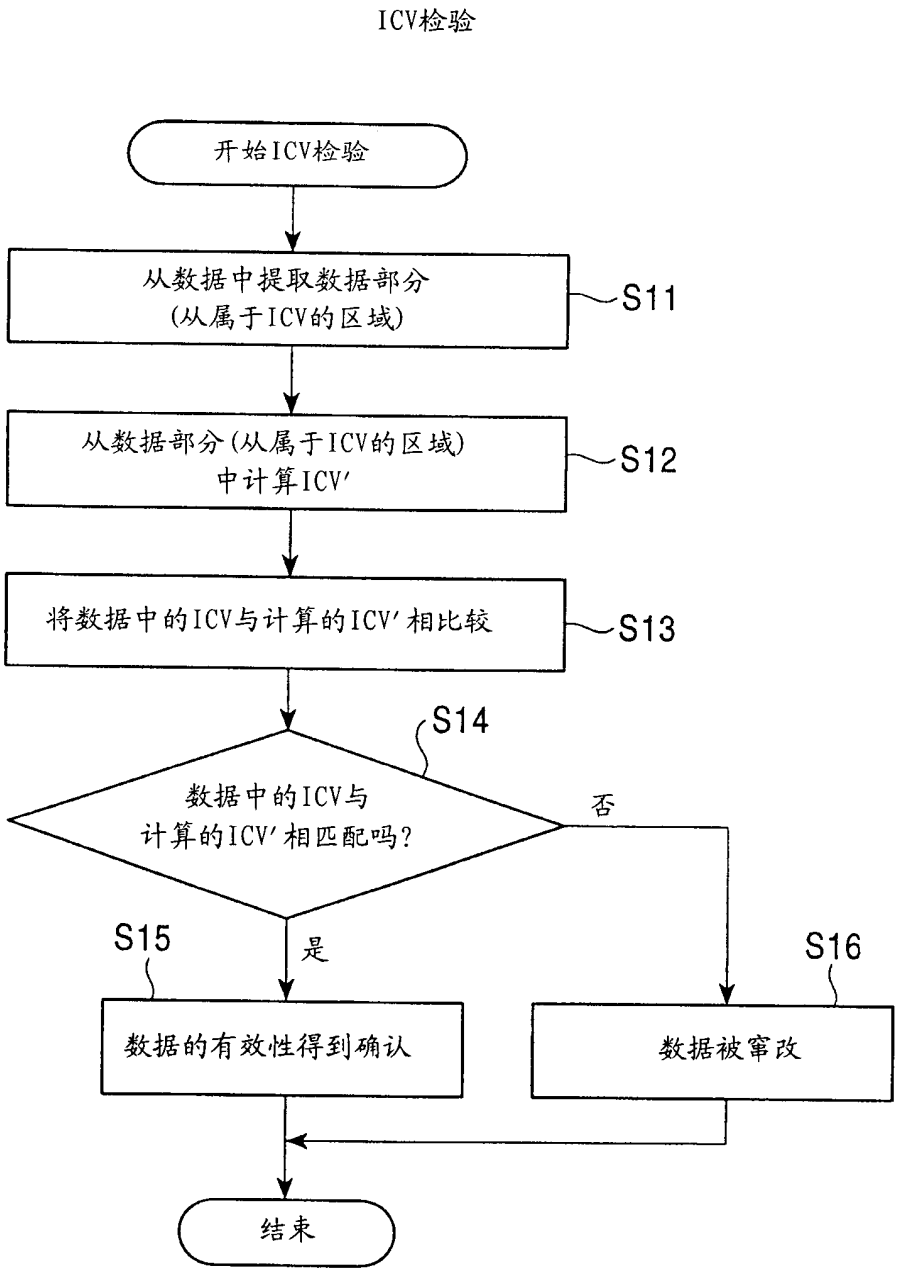

ICV检验
开始ICV检验
从数据中提取数据部分
(从属于ICV的区域)
S11
从数据部分(从属于ICV的区域)
中计算ICV′
S12
将数据中的ICV与计算的ICV′相比较
S13
S14
数据中的ICV与
计算的ICV′相匹配吗?
否
是
S15
S16
数据的有效性得到确认
数据被窜改
结束

图 15

在启动设备时的流程

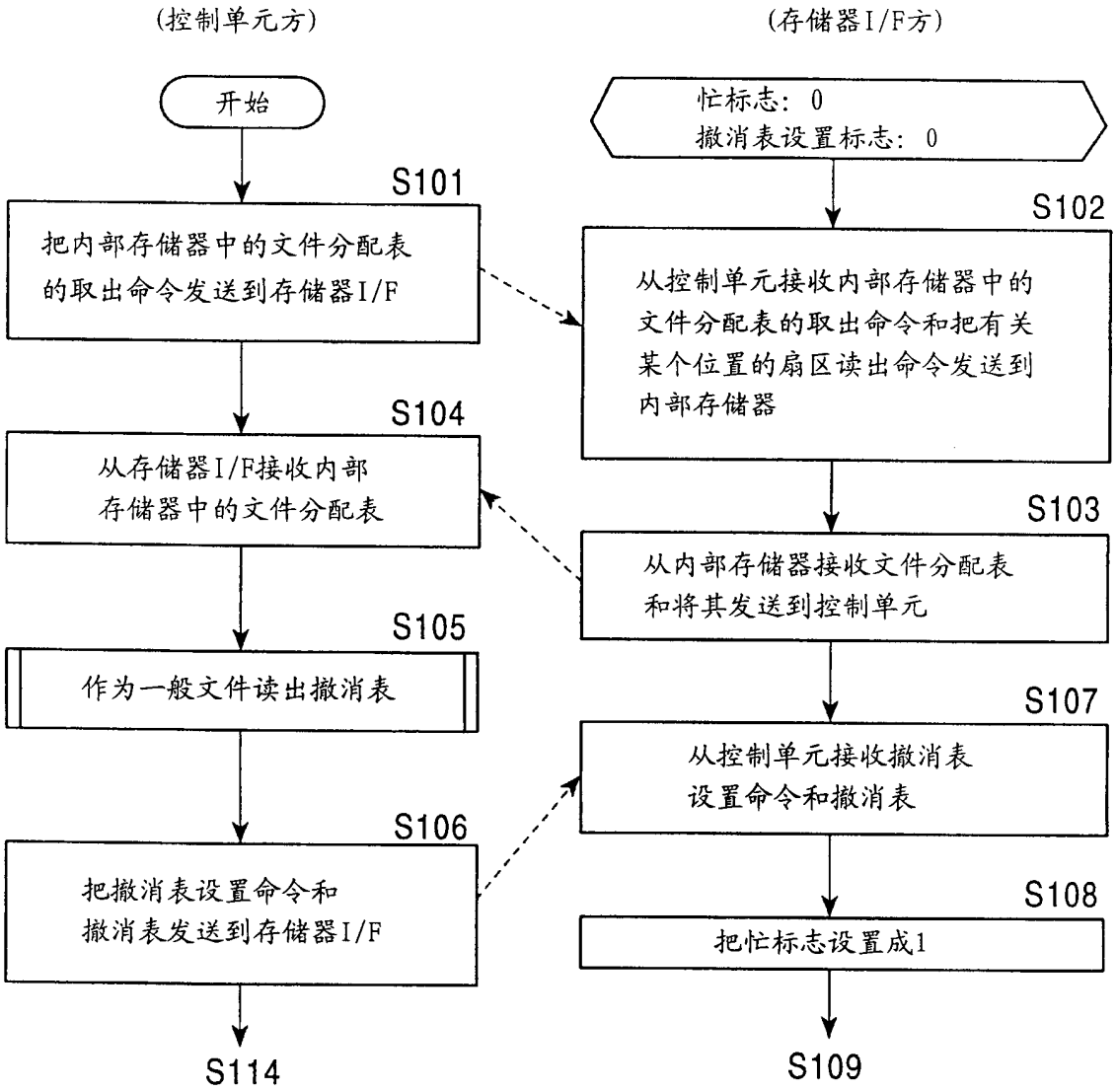


图 16-1

在启动设备时的流程

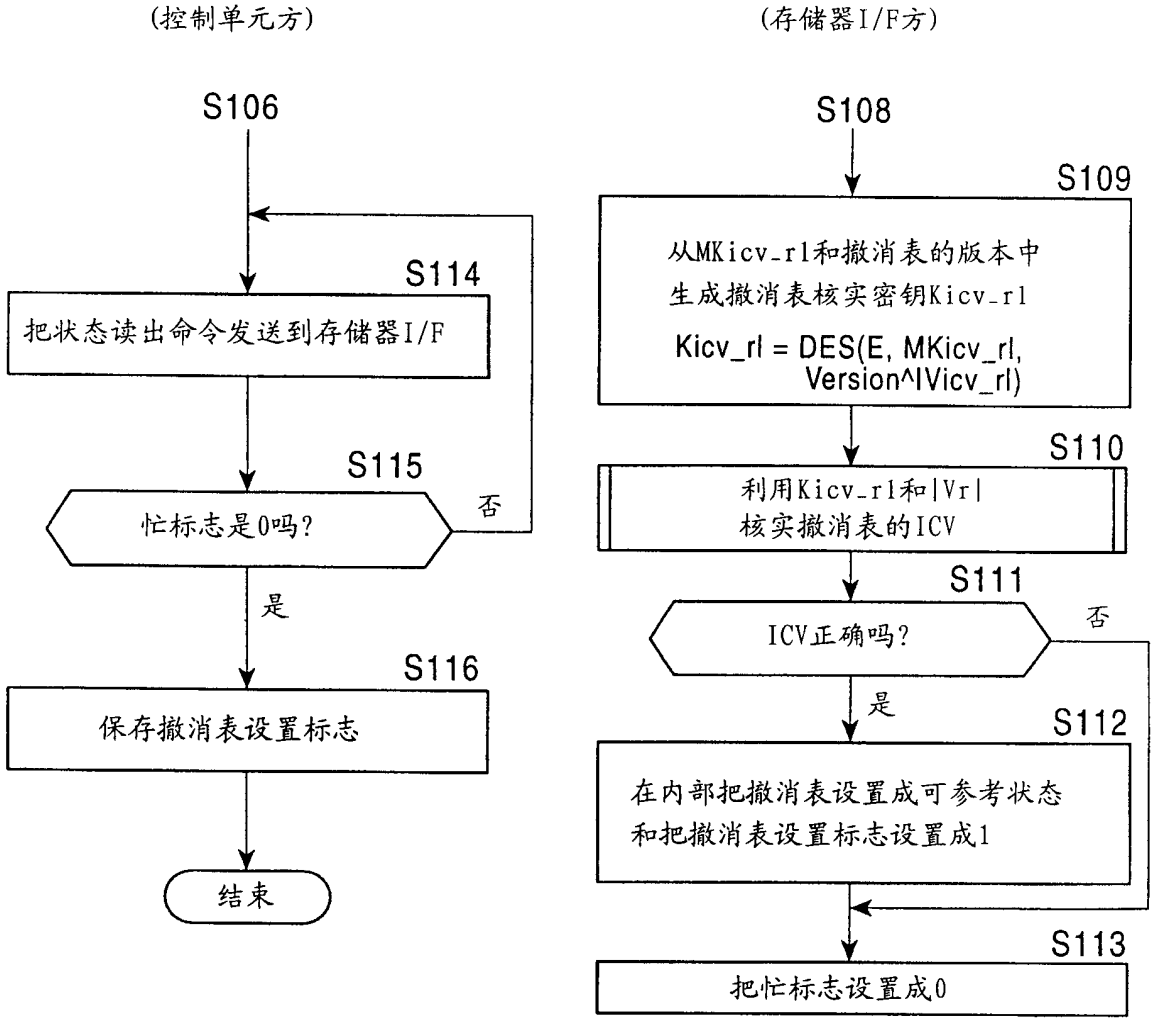


图 16-2

目录	文件名	存储扇区
/	A.h	1 - 10
/	A.cont	21 - 100
/ dir_a	B.h	101 - 110
/ dir_a	B.cont	111 - 350
/ dir_a/ dir_x	C	401 - 450
/ dir_b	D	501 - 580
/ dir_c	E.h	601 - 610
:	:	:
/ dir_c	Z.cont	5001 - 5340

图 17

在识别介质1时的流程

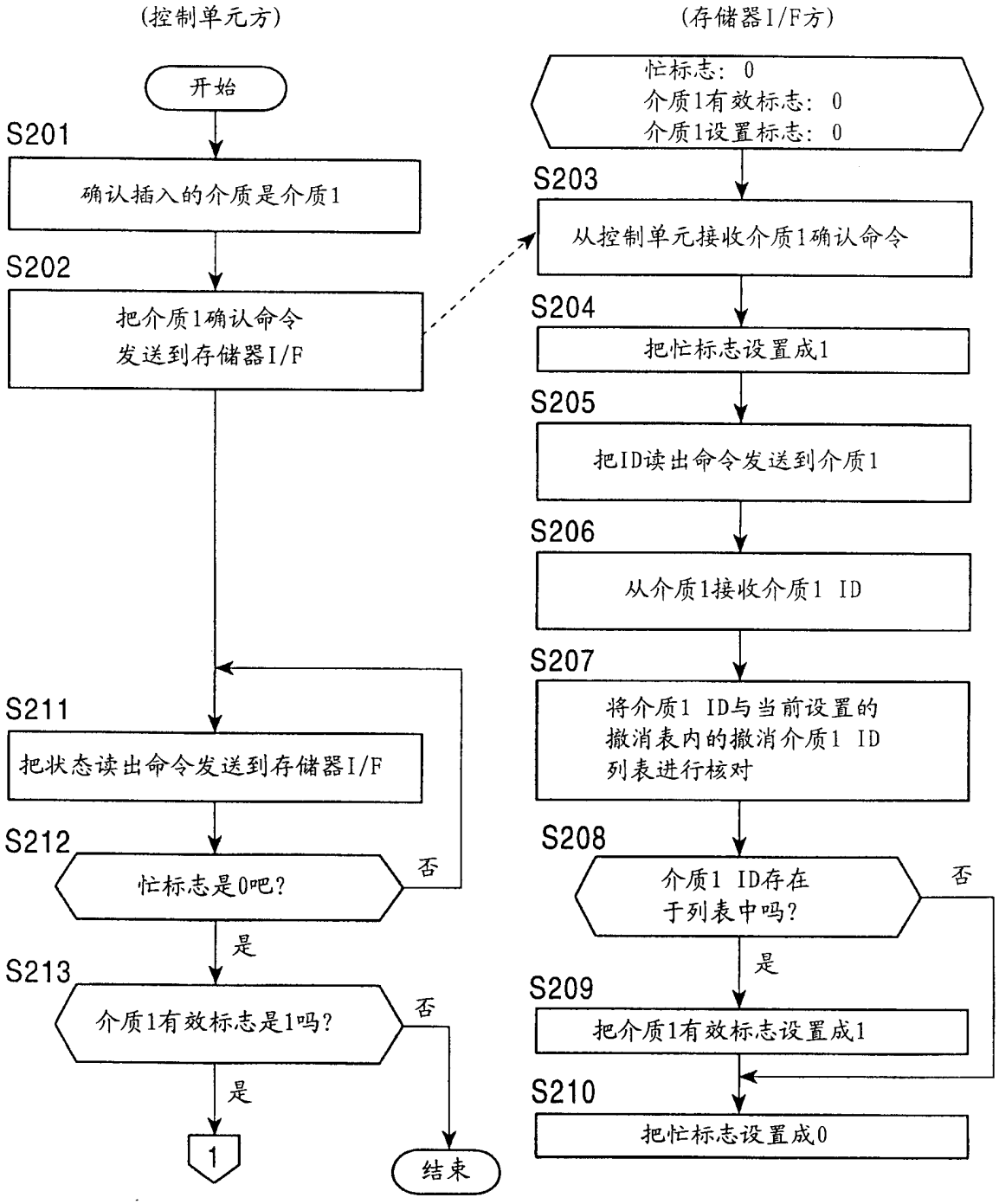


图 18

在识别介质1时的流程

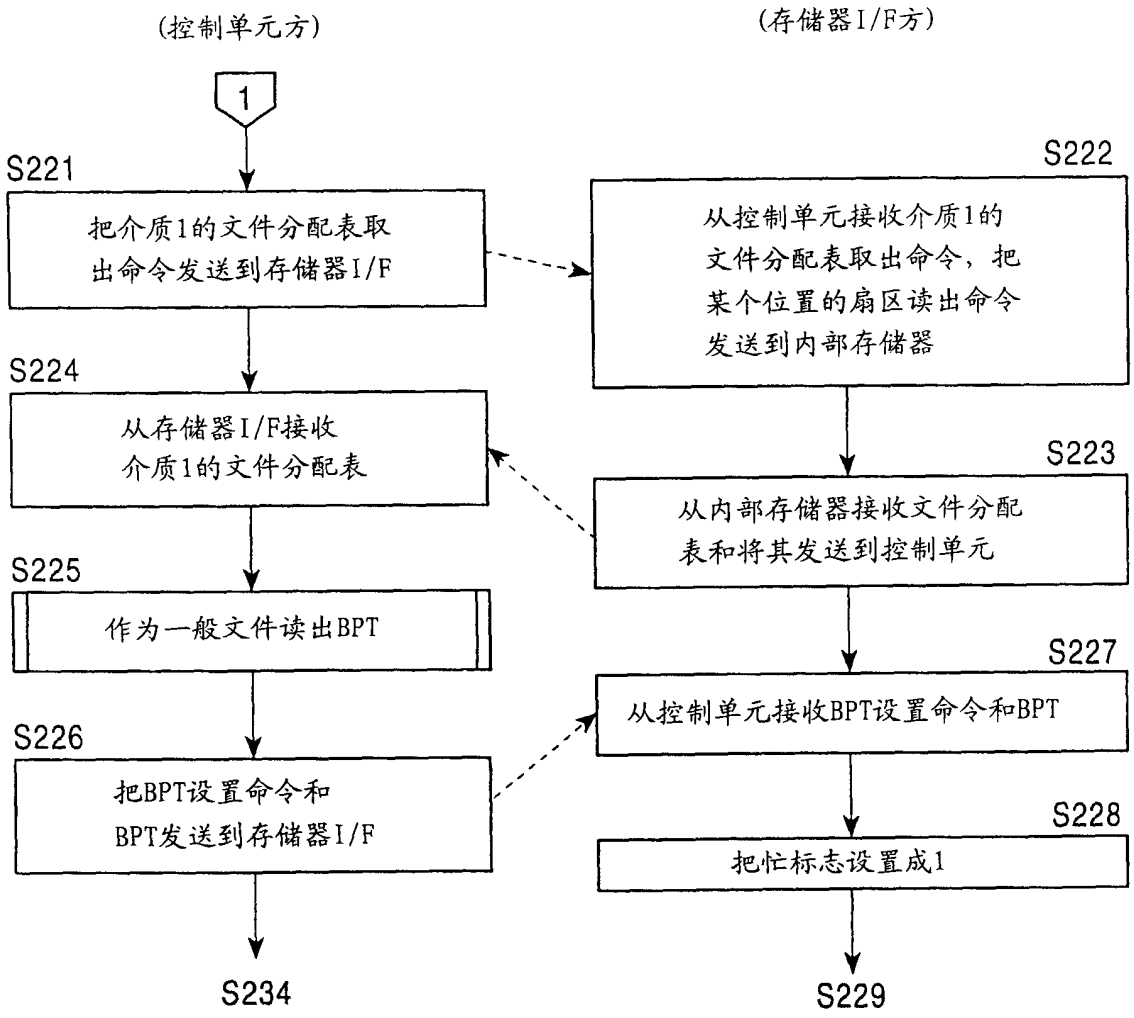


图 19-1

在识别介质1时的流程

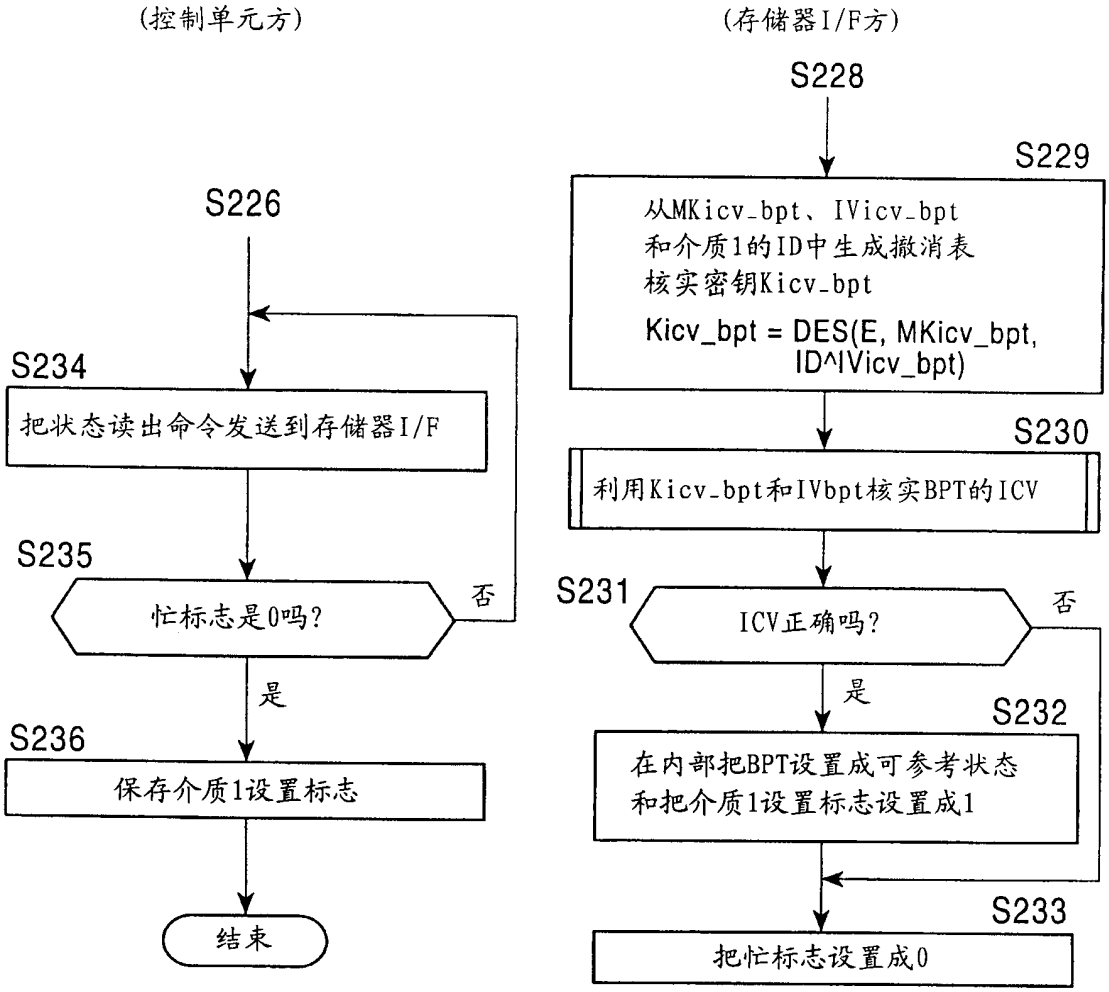


图 19-2

在识别介质2时的流程

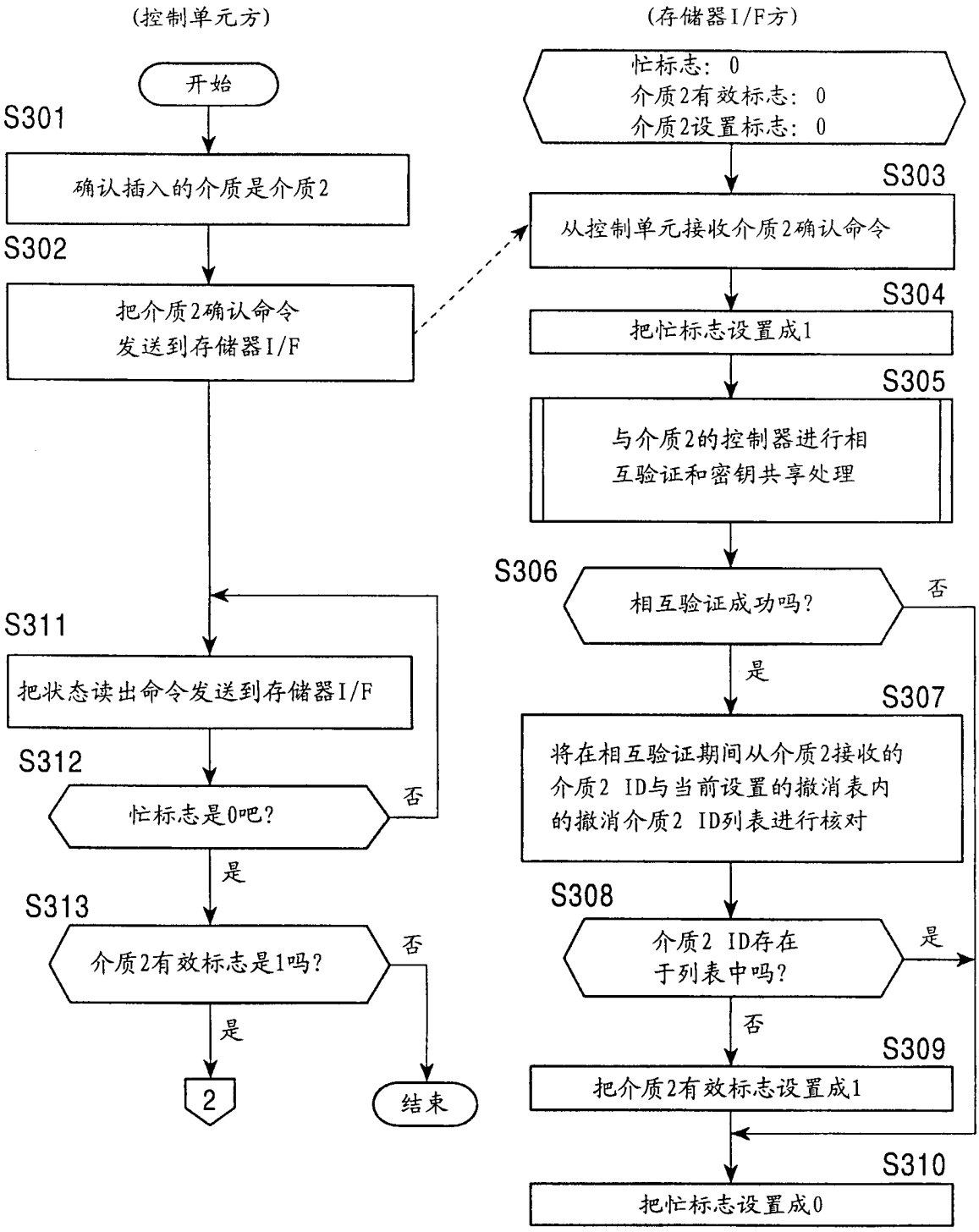


图 20

在识别介质2时的流程

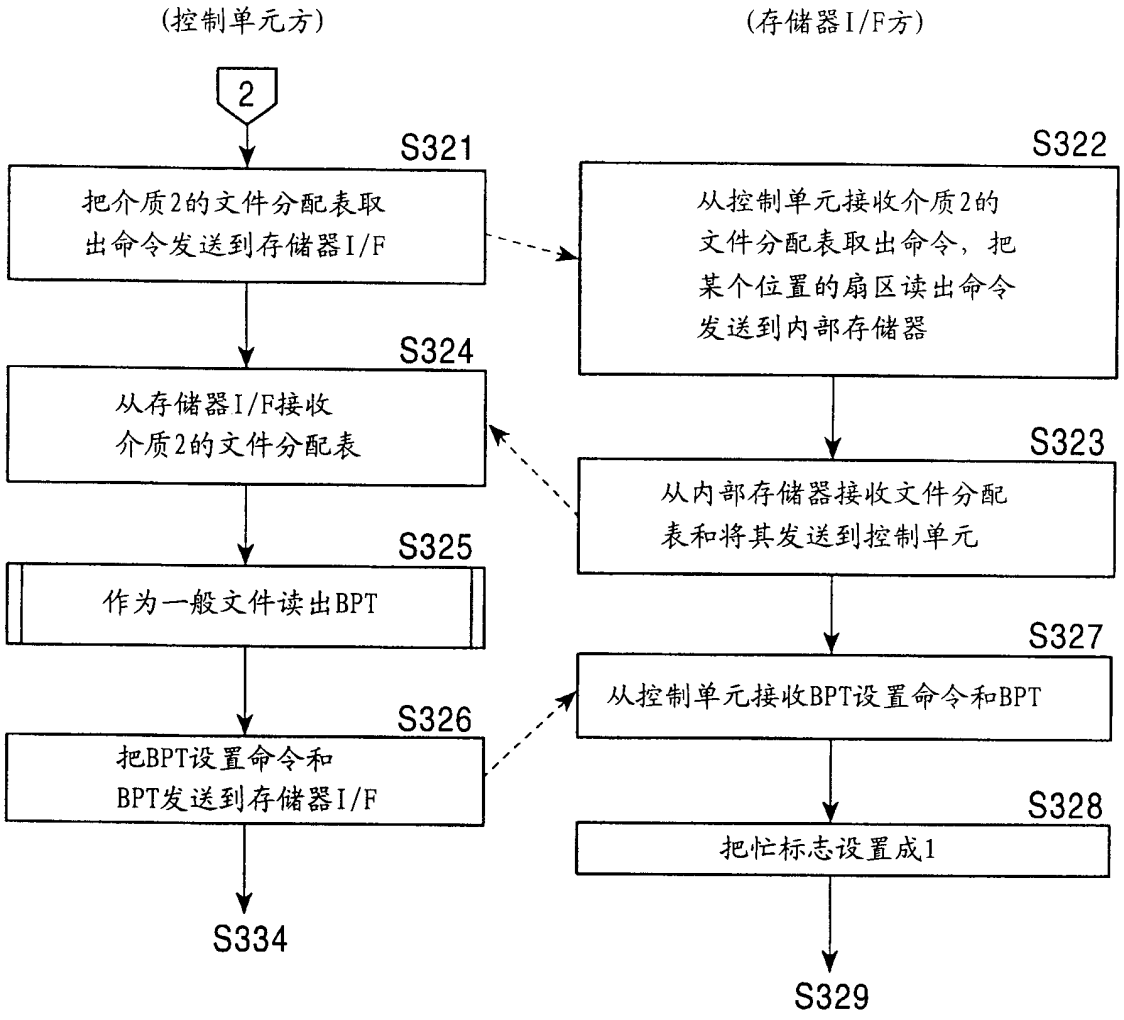


图 21-1

在识别介质2时的流程

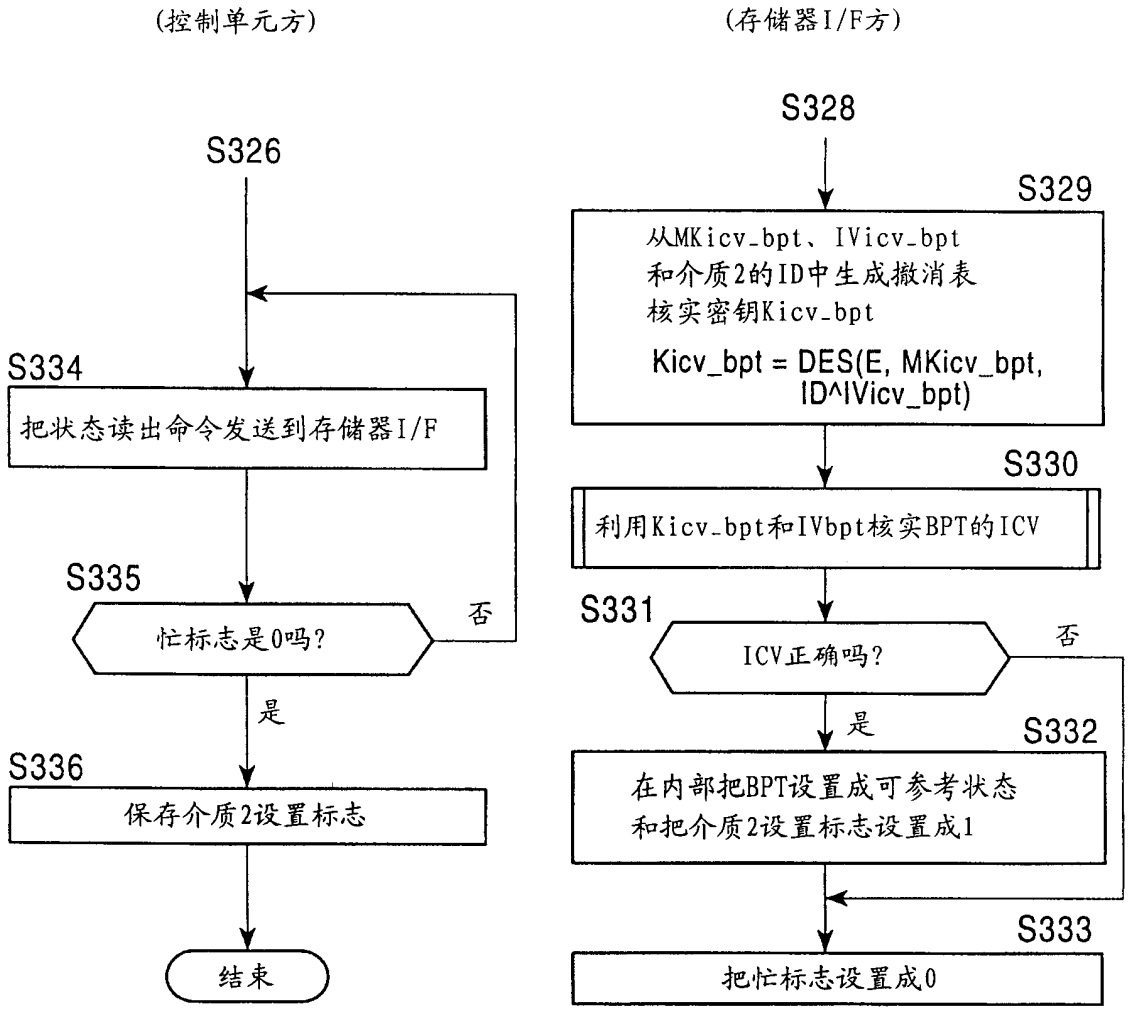


图 21-2

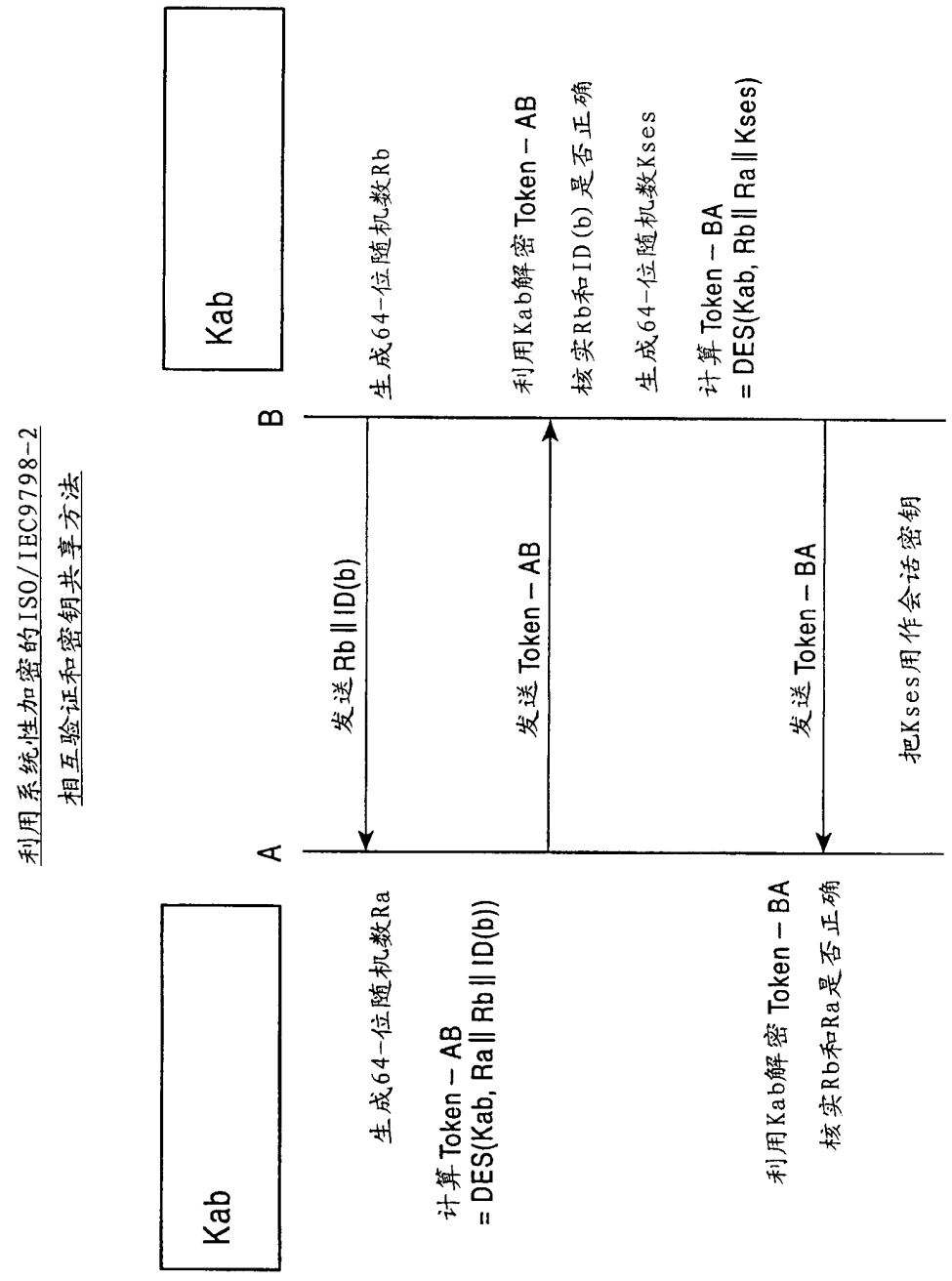

利用系统性加密的ISO/IEC9798-2
相互验证和密钥共享方法
Kab
A
生成64-位随机数Ra
计算Token－AB
= DES(Kab, Ra‖Rb‖ID(b))
发送 Rb‖ID(b)
发送 Token－AB
利用Kab解密Token－BA
核实Rb和Ra是否正确
Kab
B
生成64-位随机数Rb
利用Kab解密 Token－AB
核实Rb和ID(b)是否正确
生成64-位随机数Kses
计算 Token－BA
= DES(Kab, Rb‖Ra‖Kses)
发送 Token－BA
把Kses用作会话密钥

图 22

相互验证/密钥共享流程(续)

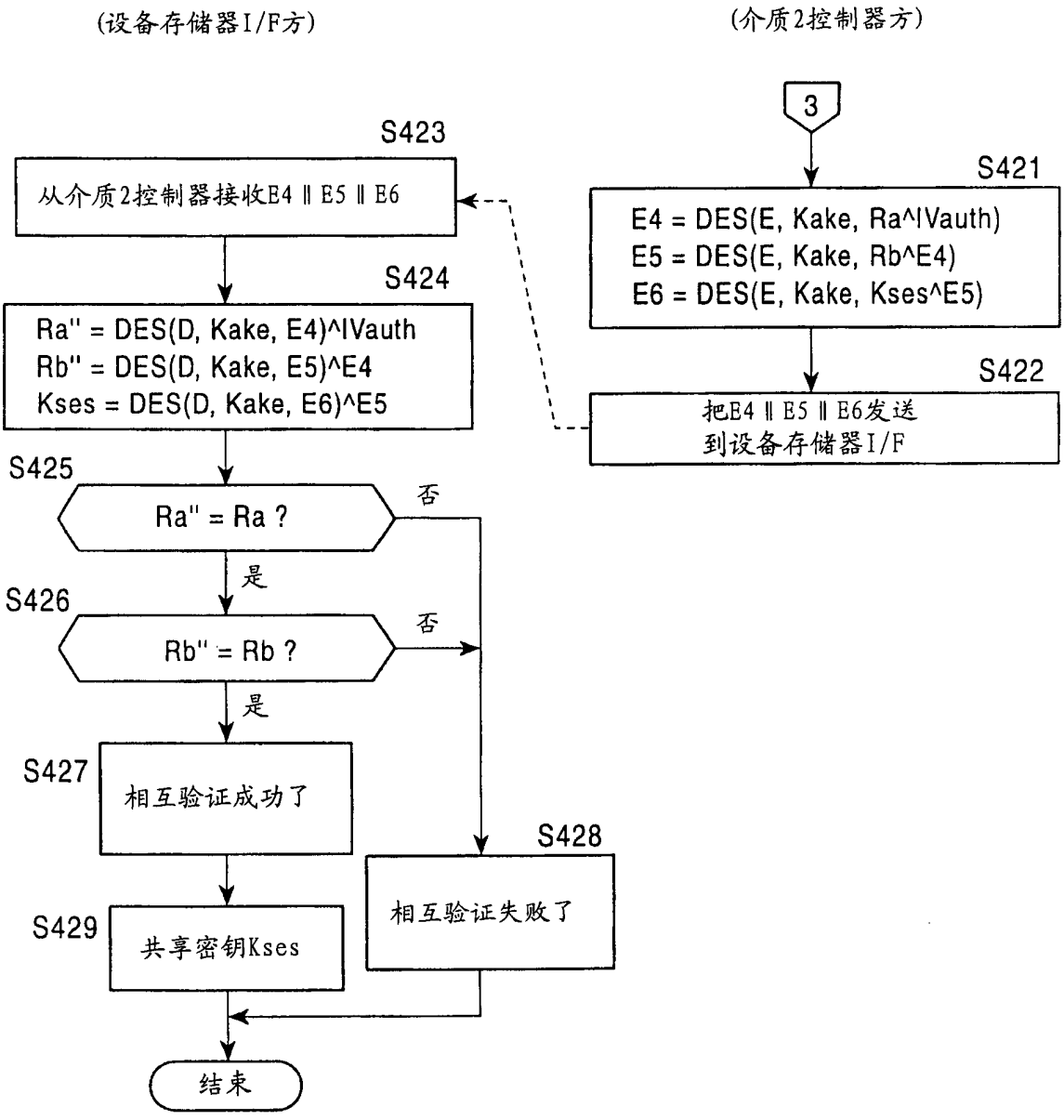


图 24

相互验证和密钥共享流程

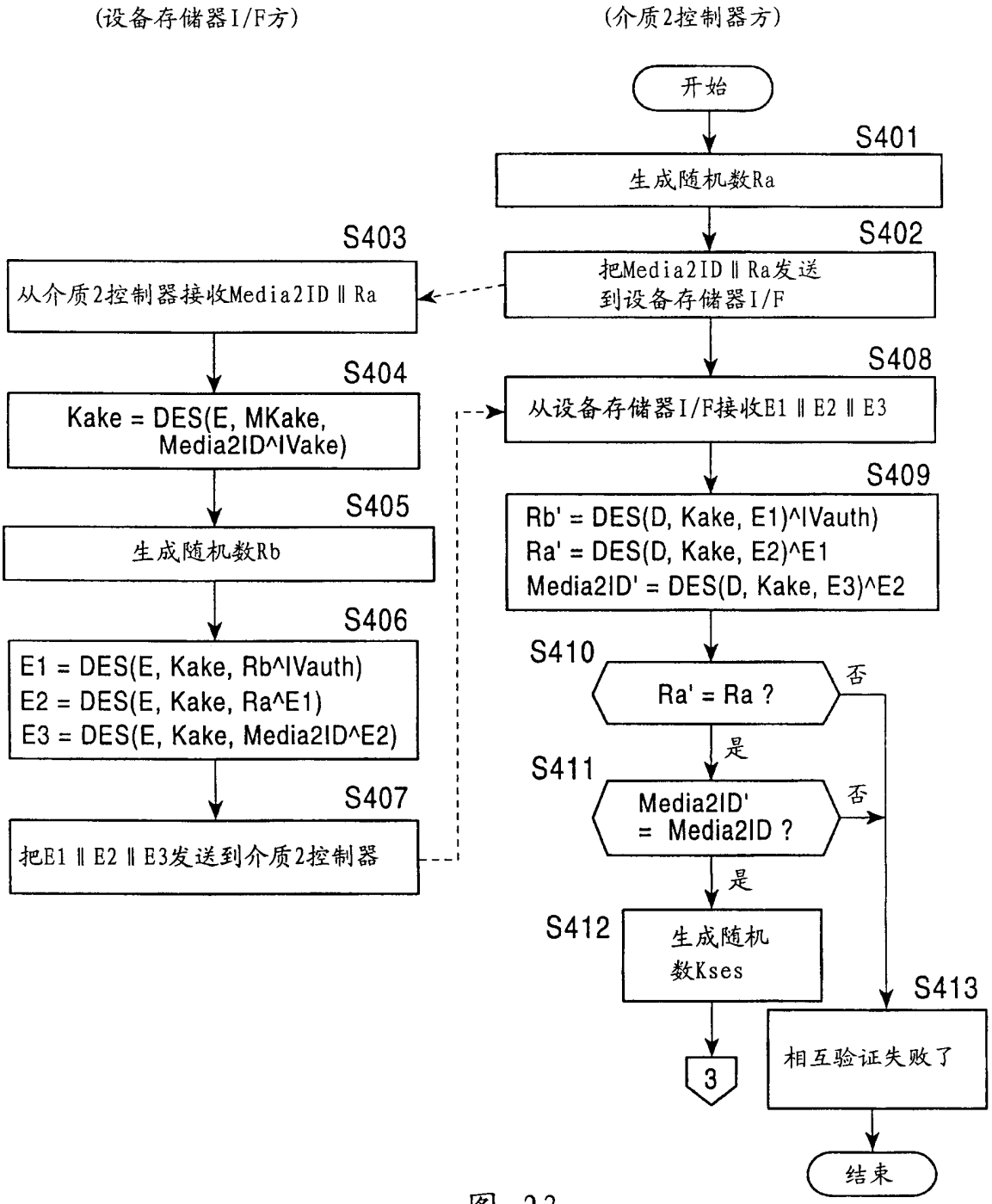


图 23

文件读出处理

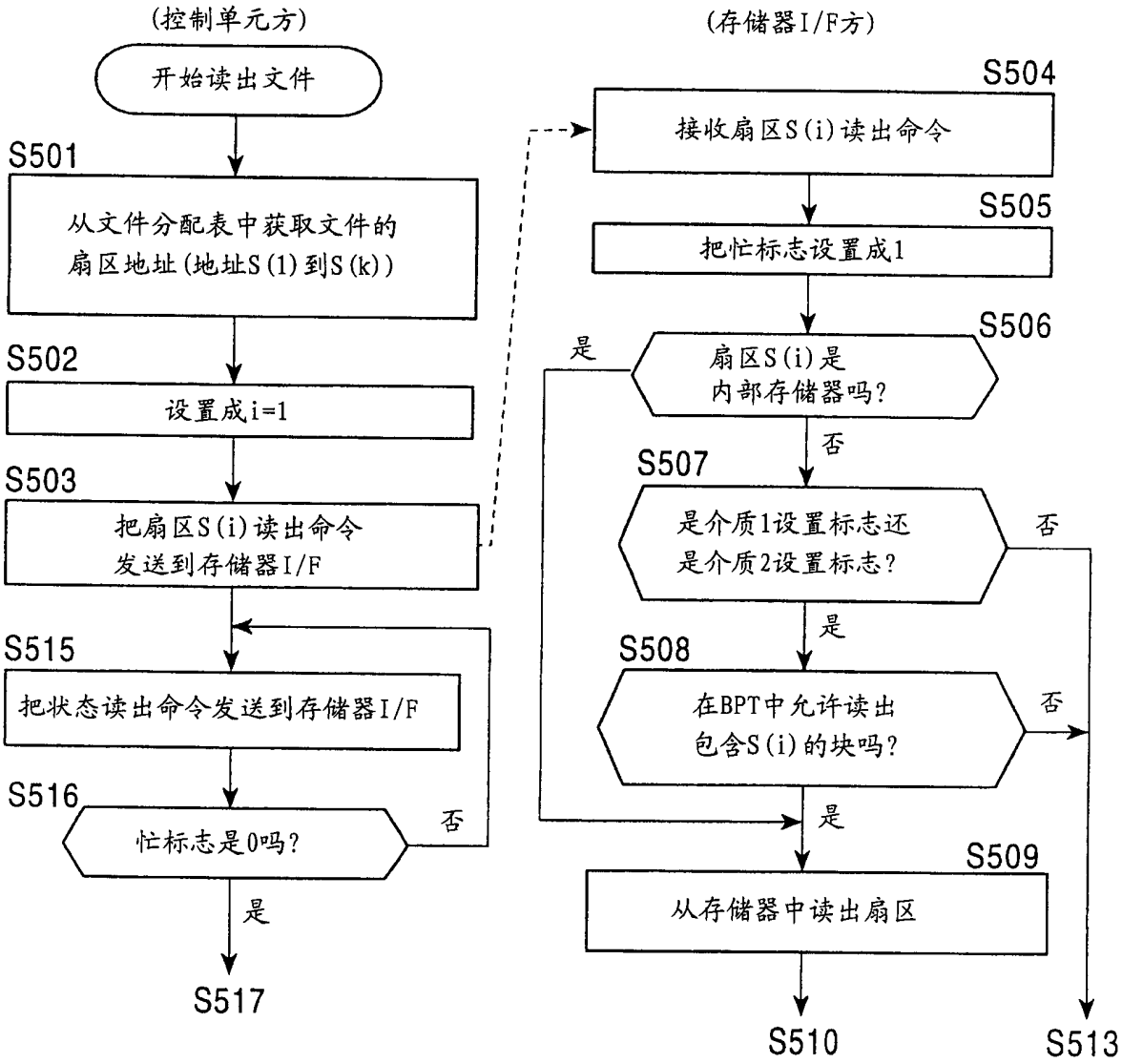

(控制单元方)
开始读出文件
S501
从文件分配表中获取文件的
扇区地址(地址S(1)到S(k))
S502
设置成i=1
S503
把扇区S(i)读出命令
发送到存储器I/F
S515
把状态读出命令发送到存储器I/F
S516
忙标志是0吗?
否
是
S517
(存储器I/F方)
S504
接收扇区S(i)读出命令
S505
把忙标志设置成1
S506
扇区S(i)是
内部存储器吗?
是
否
S507
是介质1设置标志还
是介质2设置标志?
否
是
S508
在BPT中允许读出
包含S(i)的块吗?
否
是
S509
从存储器中读出扇区
S510
S513

图 25-1

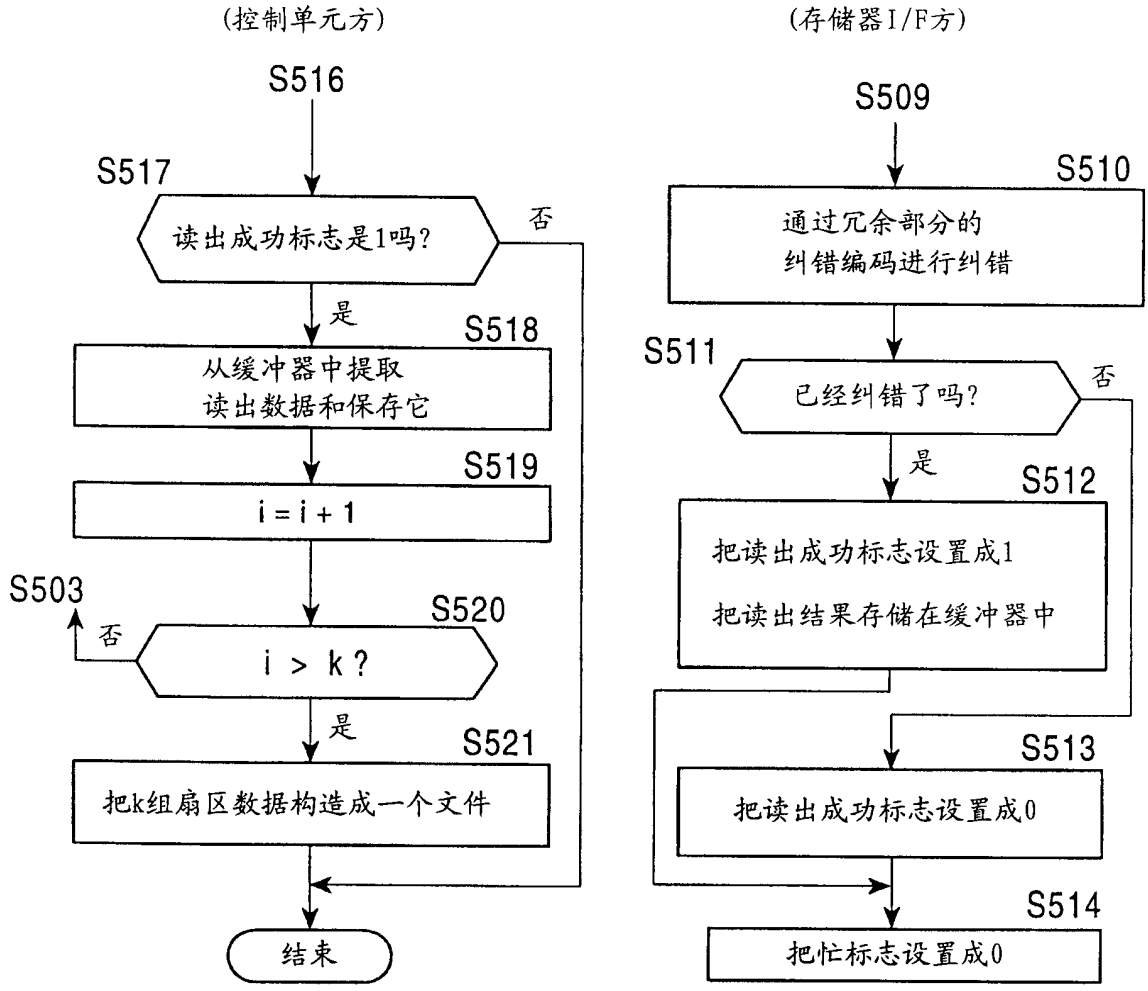

文件读出处理
(控制单元方)
(存储器I/F方)
S516
S517
读出成功标志是1吗?
否
是
S518
从缓冲器中提取
读出数据和保存它
S519
i = i + 1
S503
否
S520
i > k ?
是
S521
把k组扇区数据构造成一个文件
结束
S509
S510
通过冗余部分的
纠错编码进行纠错
S511
已经纠错了吗?
否
是
S512
把读出成功标志设置成1
把读出结果存储在缓冲器中
S513
把读出成功标志设置成0
S514
把忙标志设置成0

图 25-2

文件写入处理

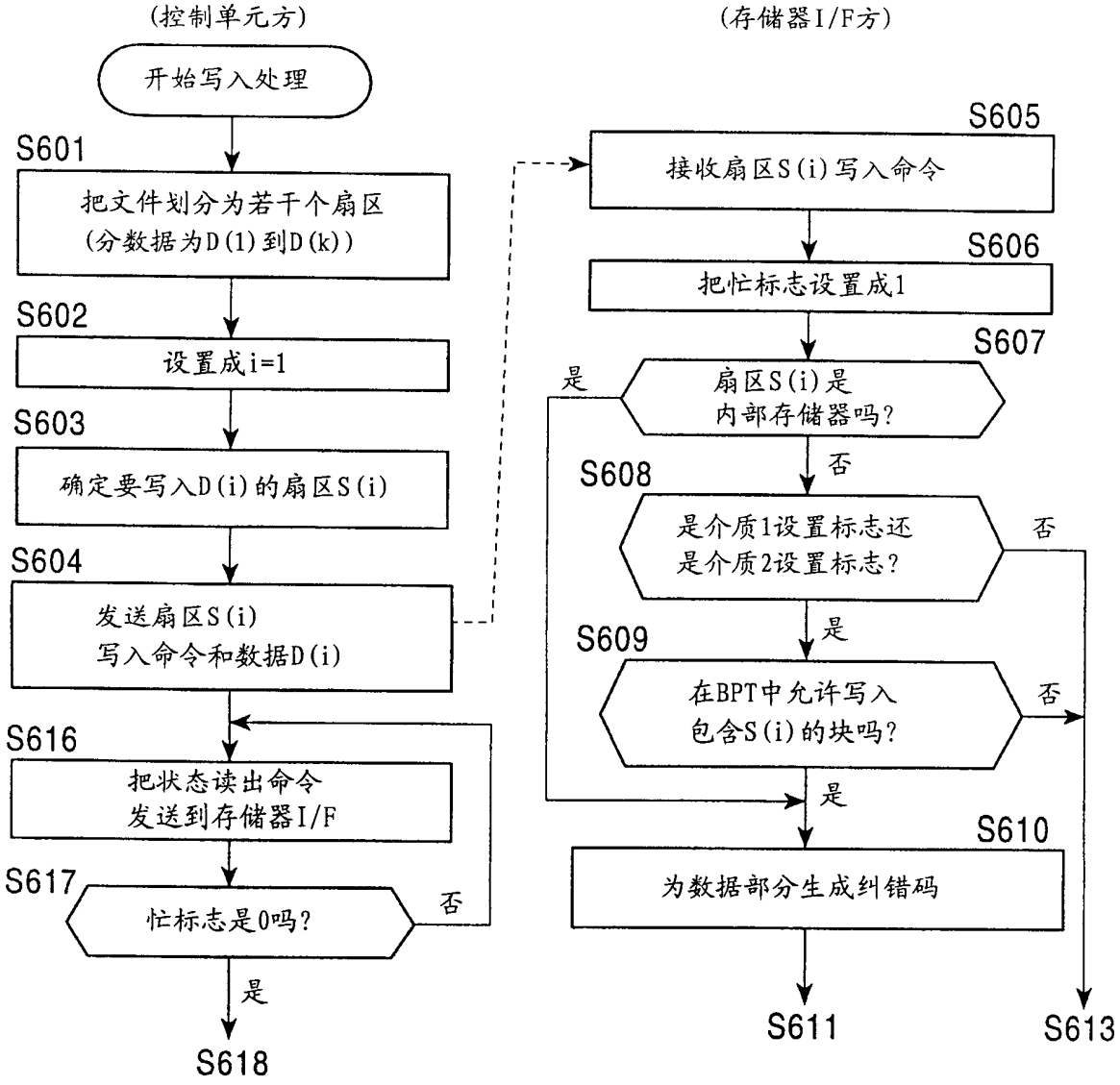

(控制单元方)
(存储器I/F方)
开始写入处理
S601
把文件划分为若干个扇区
(分数据为D(1)到D(k))
S602
设置成i=1
S603
确定要写入D(i)的扇区S(i)
S604
发送扇区S(i)
写入命令和数据D(i)
S616
把状态读出命令
发送到存储器I/F
S617
忙标志是0吗?
否
是
S618
S605
接收扇区S(i)写入命令
S606
把忙标志设置成1
S607
是
扇区S(i)是
内部存储器吗?
否
S608
是介质1设置标志还
是介质2设置标志?
否
是
S609
在BPT中允许写入
包含S(i)的块吗?
否
是
S610
为数据部分生成纠错码
S611
S613

图 26-1

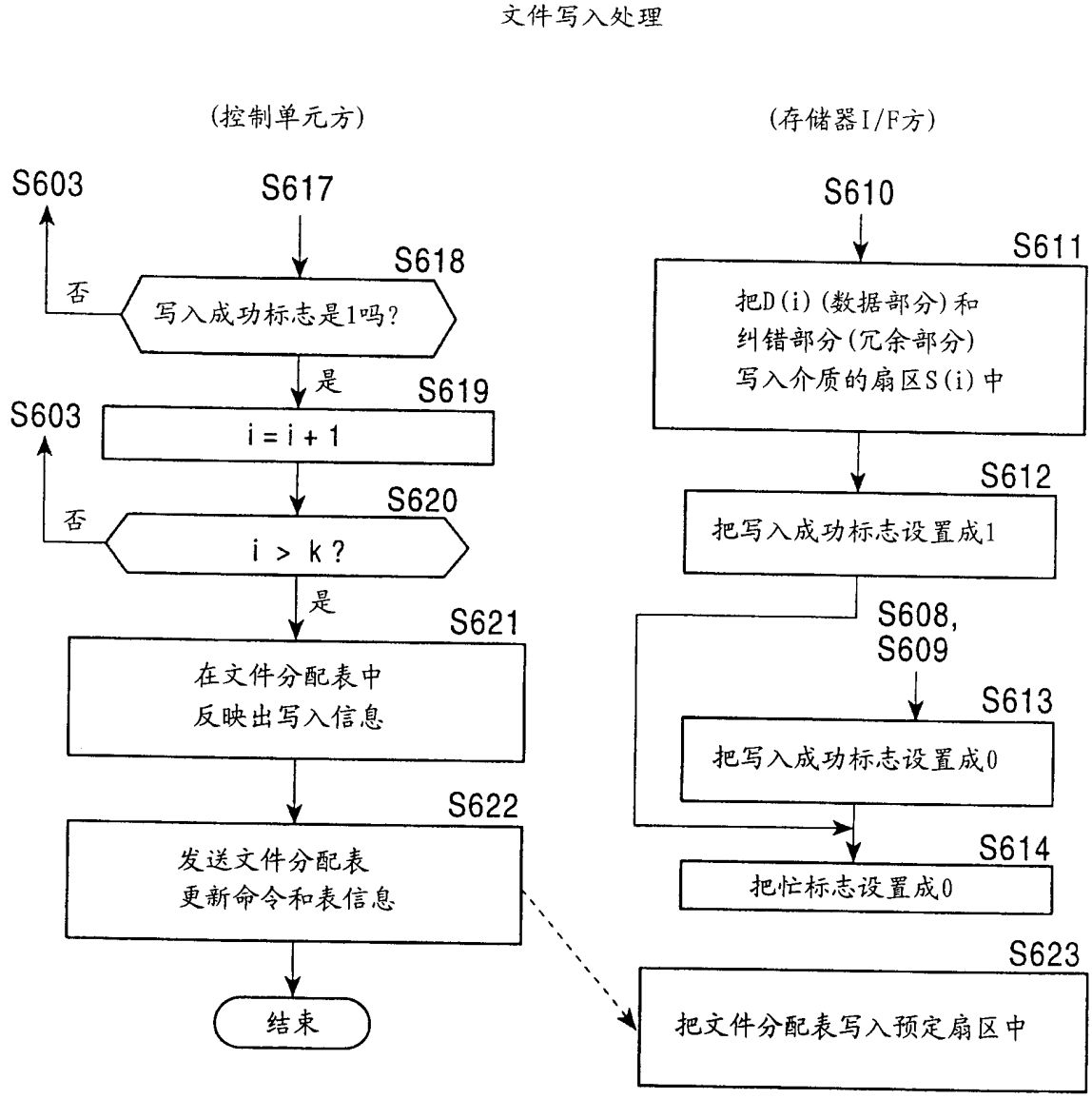

文件写入处理
(控制单元方)
(存储器I/F方)
S603
S617
S618
否
写入成功标志是1吗?
是
S619
S603
i = i + 1
否
S620
i > k ?
是
S621
在文件分配表中
反映出写入信息
S622
发送文件分配表
更新命令和表信息
结束
S610
S611
把D(i)(数据部分)和
纠错部分(冗余部分)
写入介质的扇区S(i)中
S612
把写入成功标志设置成1
S608,
S609
S613
把写入成功标志设置成0
S614
把忙标志设置成0
S623
把文件分配表写入预定扇区中

图 26-2

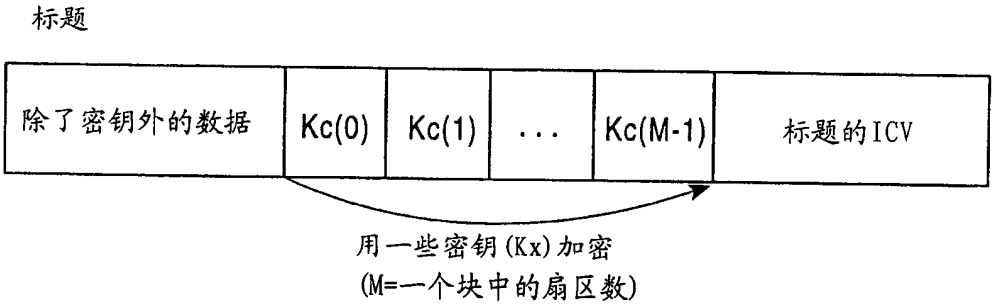

标题
除了密钥外的数据
Kc(0)
Kc(1)
...
Kc(M-1)
标题的ICV
用一些密钥(Kx)加密
(M=一个块中的扇区数)

图 27a

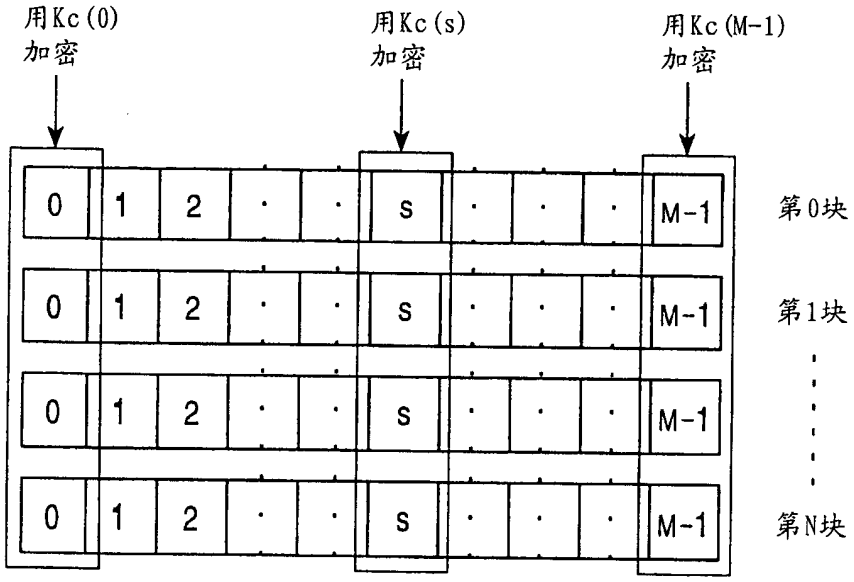

用Kc(0)
加密
用Kc(s)
加密
用Kc(M-1)
加密
0
1
2
s
M-1
第0块
第1块
第N块

图 27b

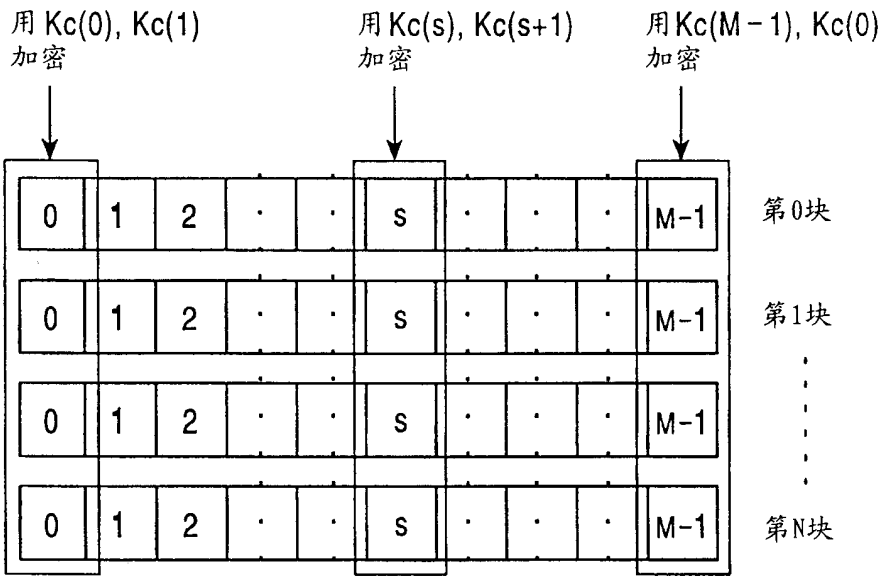


图 29

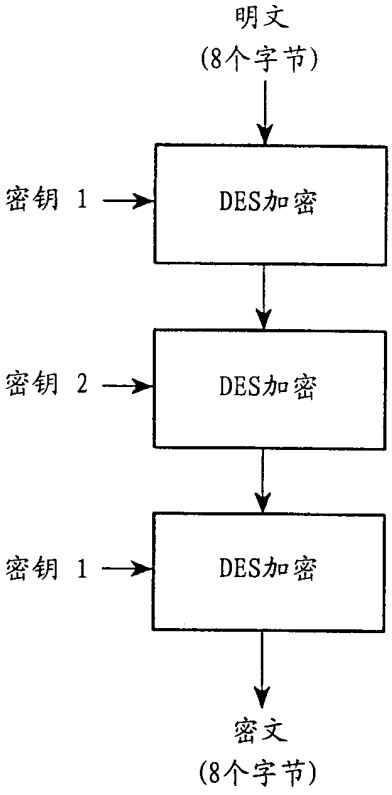

明文
(8个字节)
密钥 1
DES加密
密钥 2
DES加密
密钥 1
DES加密
密文
(8个字节)

图 28a

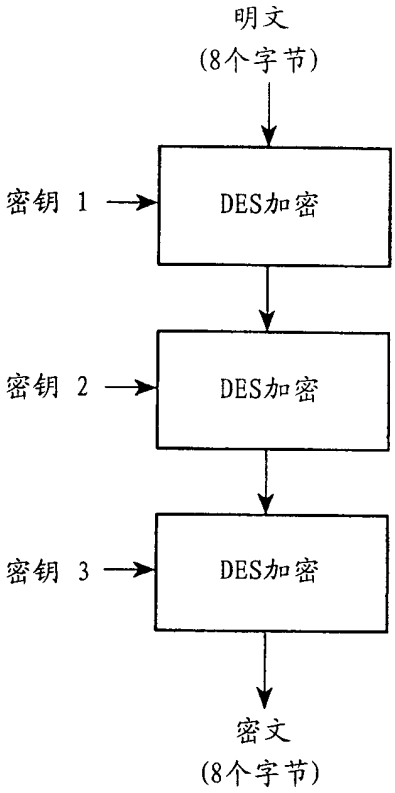

明文
(8个字节)
密钥 1
DES加密
密钥 2
DES加密
密钥 3
DES加密
密文
(8个字节)

图 28b

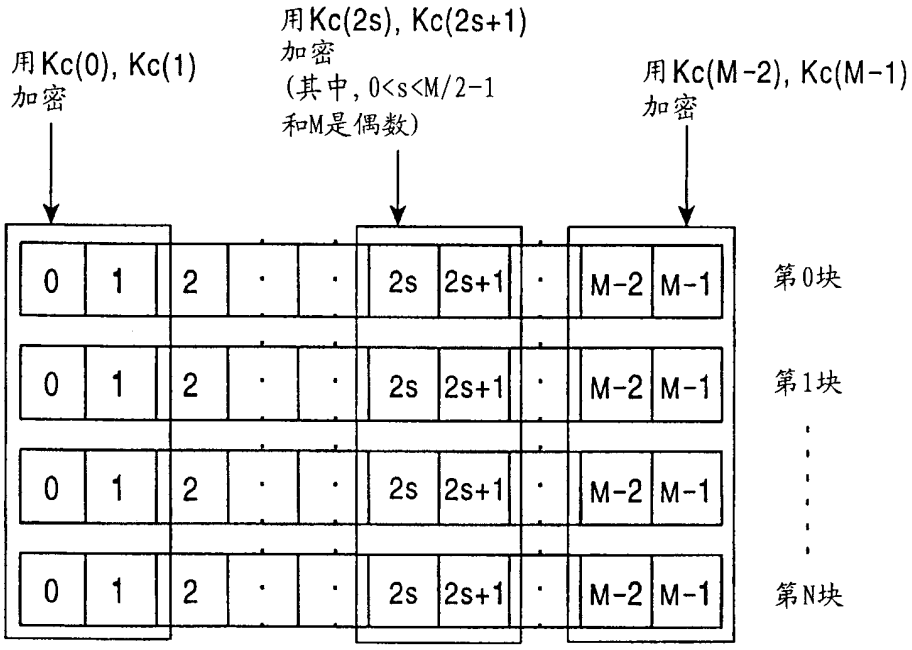

用Kc(0), Kc(1)
加密
用Kc(2s), Kc(2s+1)
加密
(其中, 0<s<M/2-1
和M是偶数)
用Kc(M-2), Kc(M-1)
加密
0
1
2
2s
2s+1
M-2
M-1
第0块
第1块
第N块

图 30

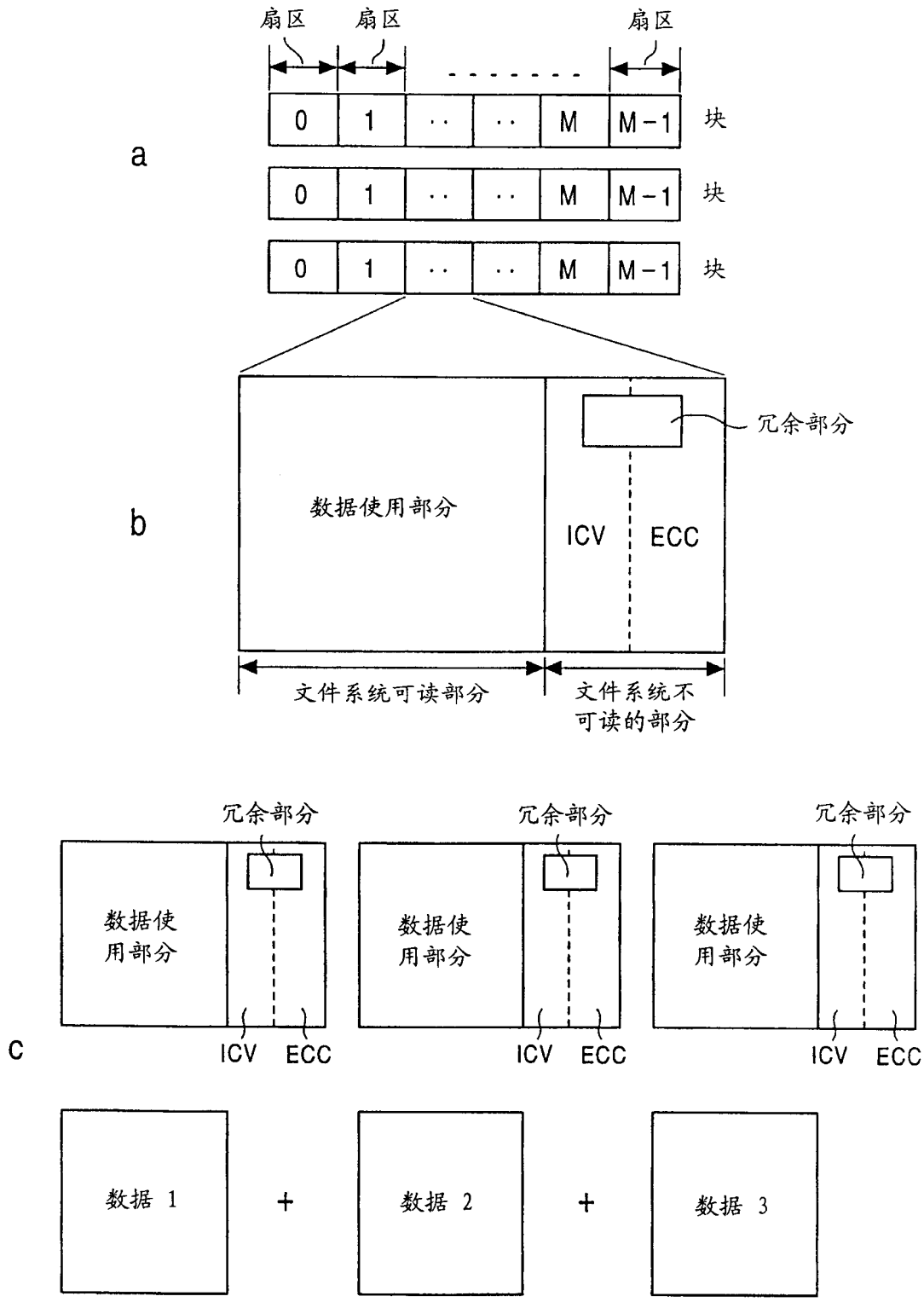

a
扇区
扇区
扇区
0
1
M
M-1
块
b
数据使用部分
ICV
ECC
冗余部分
文件系统可读部分
文件系统不
可读的部分
c
冗余部分
数据使
用部分
ICV
ECC
数据 1
+
数据 2
数据 3

图 31

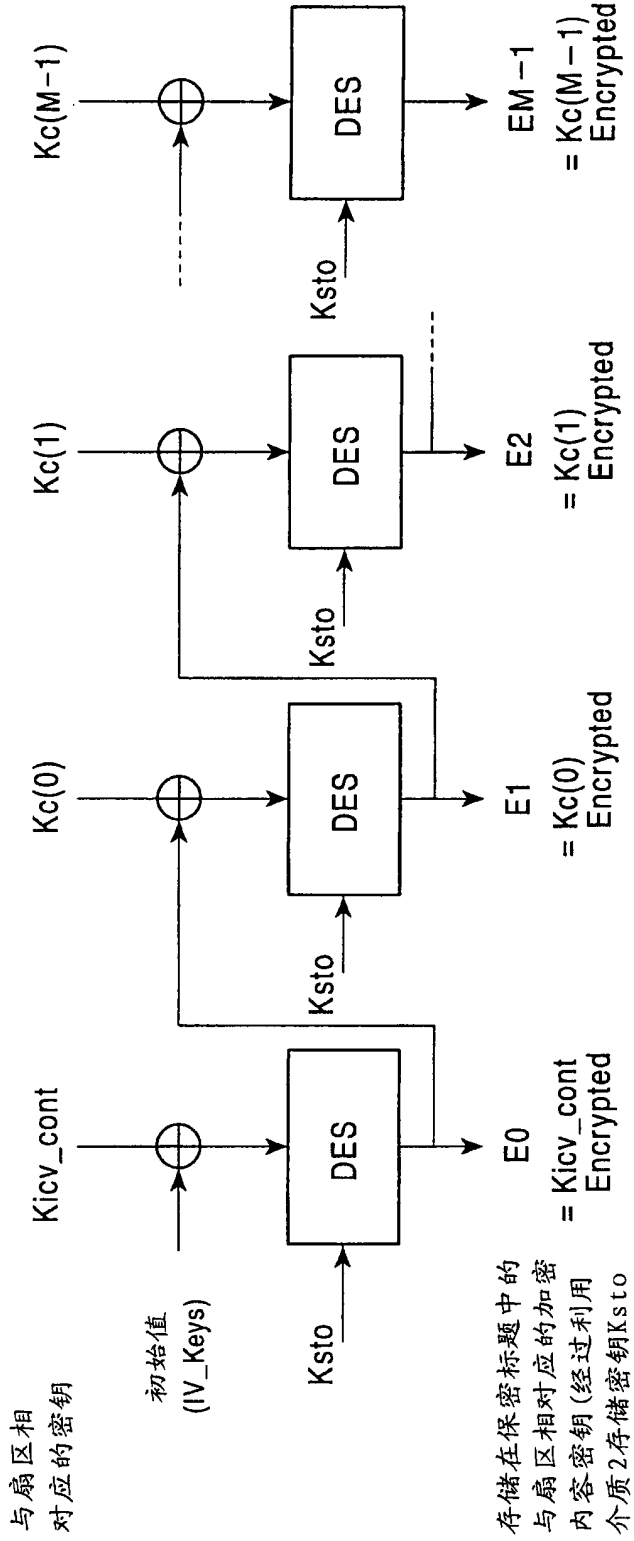

Kicv_cont
Kc(0)
Kc(1)
Kc(M-1)
DES
DES
DES
DES
Ksto
Ksto
Ksto
Ksto
初始值
(IV_Keys)
E0
= Kicv_cont
Encrypted
E1
= Kc(0)
Encrypted
E2
= Kc(1)
Encrypted
EM-1
= Kc(M-1)
Encrypted
与扇区相
对应的密钥
存储在保密标题中的
与扇区相对应的加密
内容密钥(经过利用
介质2存储密钥Ksto
的CBC模式加密)

图 32

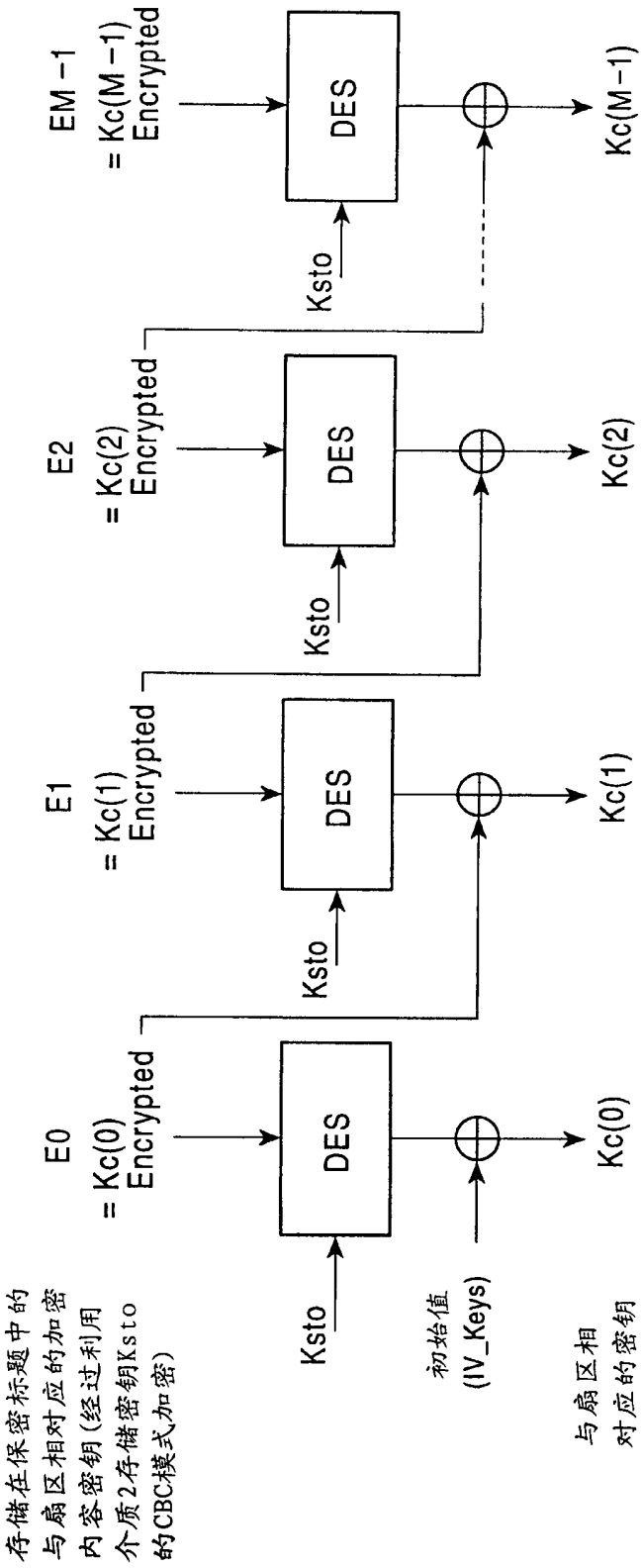

存储在保密标题中的
与扇区相对应的加密
内容密钥(经过利用
介质2存储密钥Ksto
的CBC模式加密)
E0
= Kc(0)
Encrypted
E1
= Kc(1)
Encrypted
E2
= Kc(2)
Encrypted
EM-1
= Kc(M-1)
Encrypted
DES
DES
DES
DES
Ksto
Ksto
Ksto
Ksto
初始值
(IV_Keys)
Kc(0)
Kc(1)
Kc(2)
Kc(M-1)
与扇区相
对应的密钥

图 33

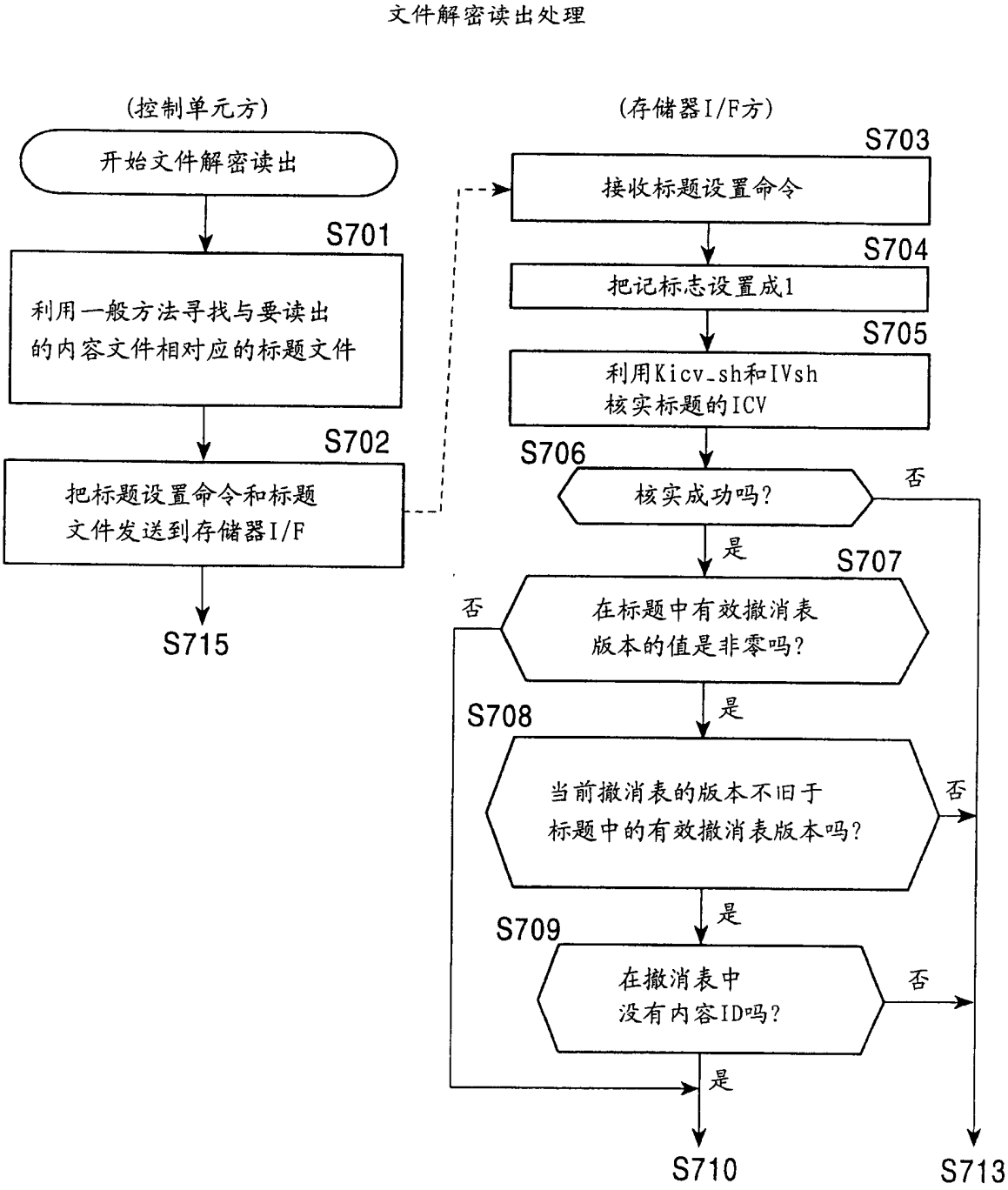

文件解密读出处理
(控制单元方)
(存储器I/F方)
开始文件解密读出
S701
利用一般方法寻找与要读出的内容文件相对应的标题文件
S702
把标题设置命令和标题文件发送到存储器I/F
S715
S703
接收标题设置命令
S704
把记标志设置成1
S705
利用Kicv_sh和IVsh核实标题的ICV
S706
核实成功吗?
否
是
S707
在标题中有效撤消表版本的值是非零吗?
否
是
S708
当前撤消表的版本不旧于标题中的有效撤消表版本吗?
否
是
S709
在撤消表中没有内容ID吗?
否
是
S710
S713

图 35-1

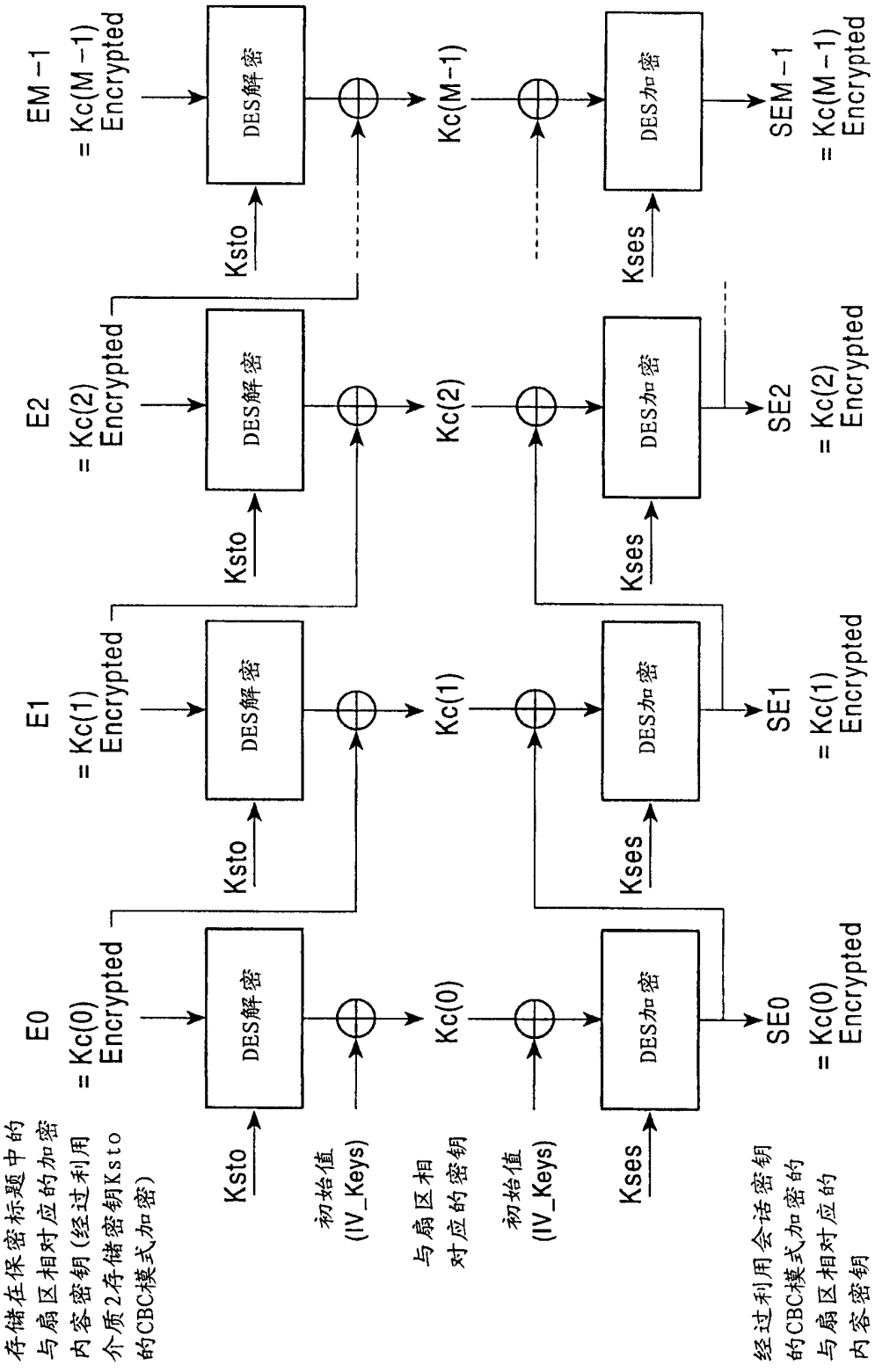

存储在保密标题中的
与扇区相对应的加密
内容密钥(经过利用
介质2存储密钥Ksto
的CBC模式加密)
E0
= Kc(0)
Encrypted
E1
= Kc(1)
Encrypted
E2
= Kc(2)
Encrypted
EM-1
= Kc(M-1)
Encrypted
Ksto
DES解密
初始值
(IV_Keys)
与扇区相
对应的密钥
Kc(0)
Kc(1)
Kc(2)
Kc(M-1)
Kses
DES加密
SE0
= Kc(0)
Encrypted
SE1
= Kc(1)
Encrypted
SE2
= Kc(2)
Encrypted
SEM-1
= Kc(M-1)
Encrypted
经过利用会话密钥
的CBC模式加密的
与扇区相对应的
内容密钥

图 34

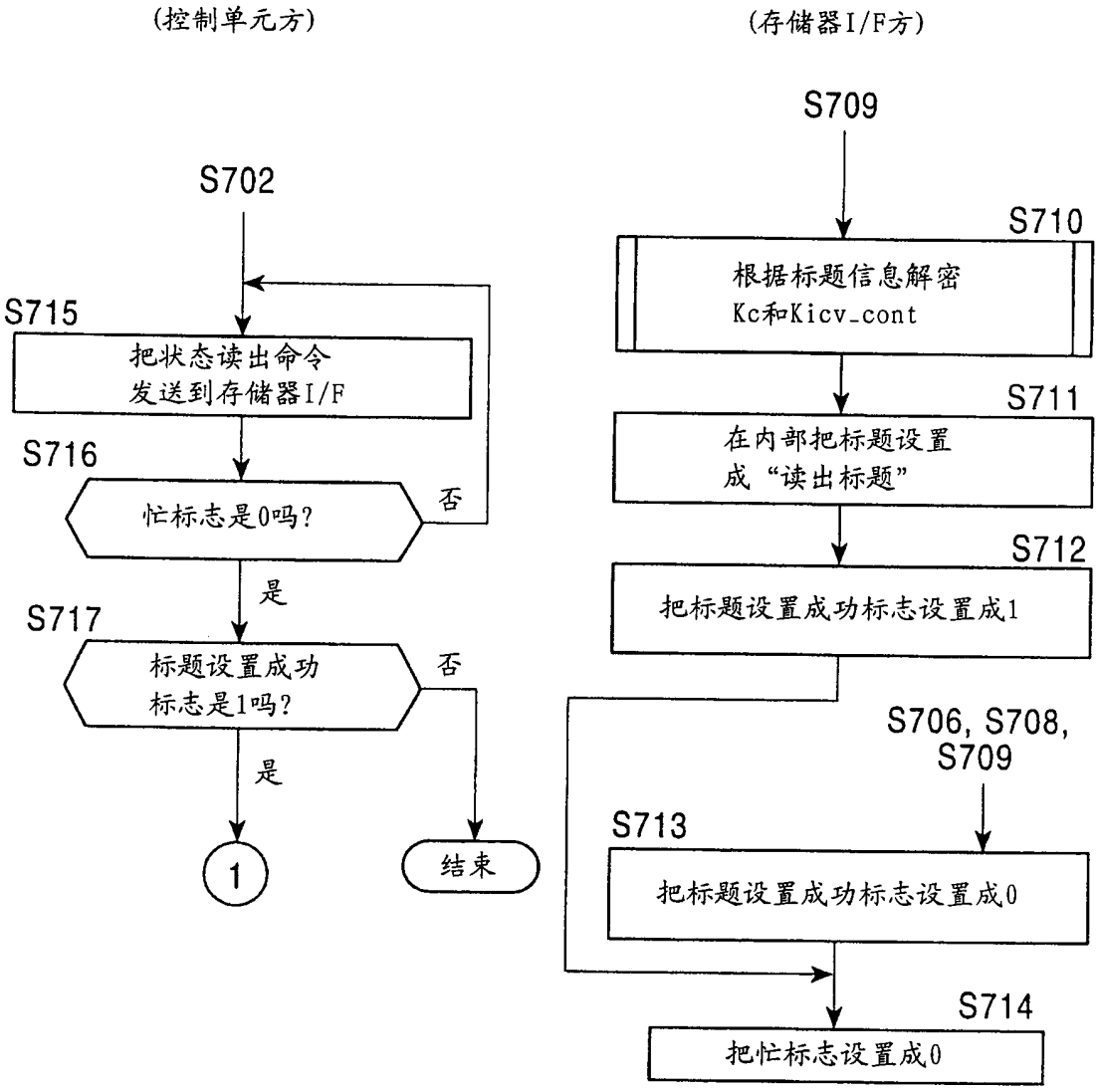

文件解密读出处理
(控制单元方)
(存储器I/F方)
S709
S702
S710
根据标题信息解密
Kc和Kicv_cont
S715
把状态读出命令
发送到存储器I/F
S711
在内部把标题设置
成“读出标题”
S716
忙标志是0吗?
否
是
S712
把标题设置成功标志设置成1
S717
标题设置成功
标志是1吗?
否
是
S706, S708,
S709
S713
把标题设置成功标志设置成0
1
结束
S714
把忙标志设置成0

图 35-2

解密读出处理

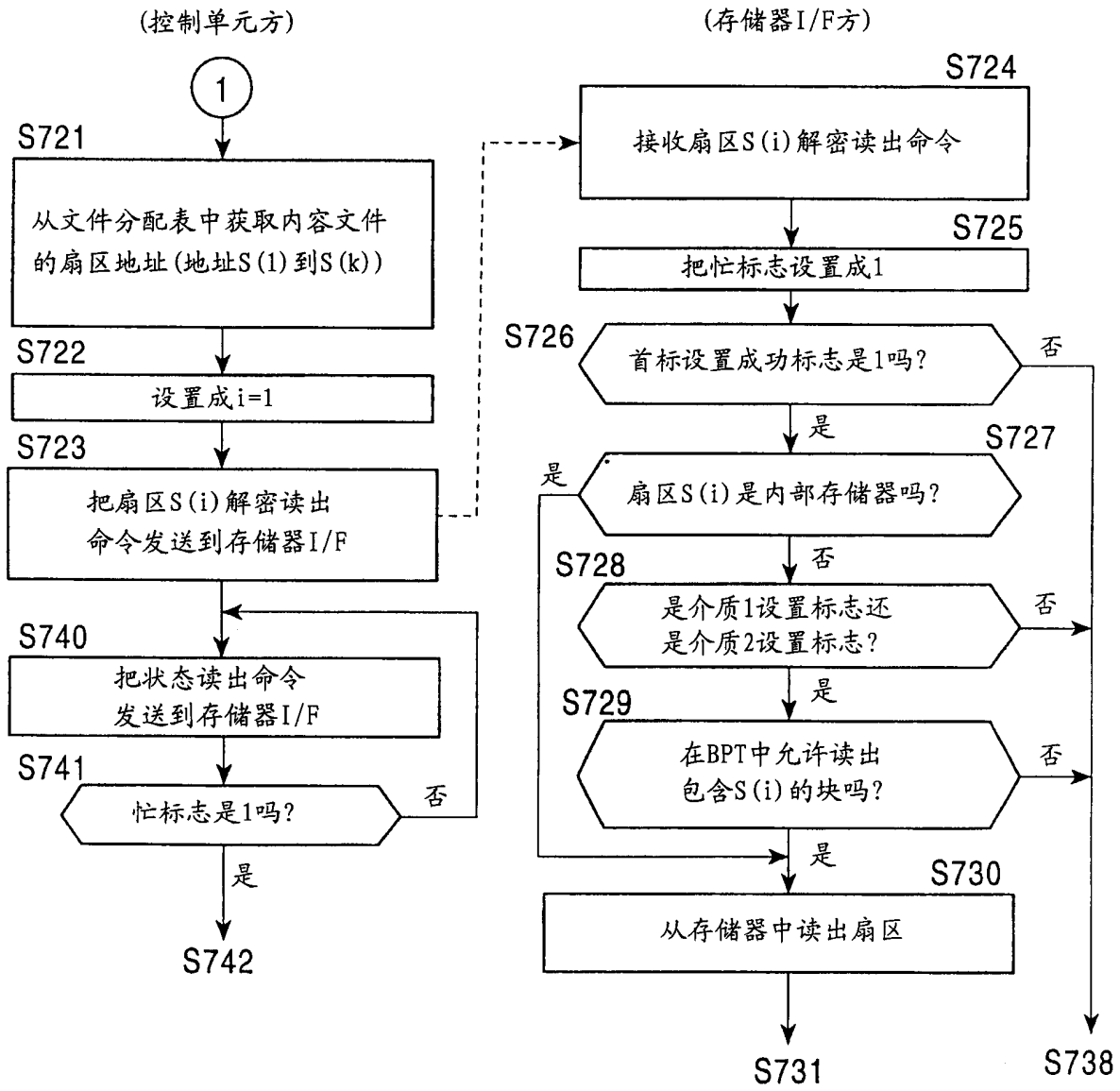

(控制单元方)
(存储器I/F方)
1
S721
从文件分配表中获取内容文件的扇区地址(地址S(1)到S(k))
S722
设置成i=1
S723
把扇区S(i)解密读出命令发送到存储器I/F
S740
把状态读出命令发送到存储器I/F
S741
忙标志是1吗?
否
是
S742
S724
接收扇区S(i)解密读出命令
S725
把忙标志设置成1
S726
首标设置成功标志是1吗?
否
是
S727
扇区S(i)是内部存储器吗?
是
否
S728
是介质1设置标志还是介质2设置标志?
否
是
S729
在BPT中允许读出包含S(i)的块吗?
否
是
S730
从存储器中读出扇区
S731
S738

图 36-1

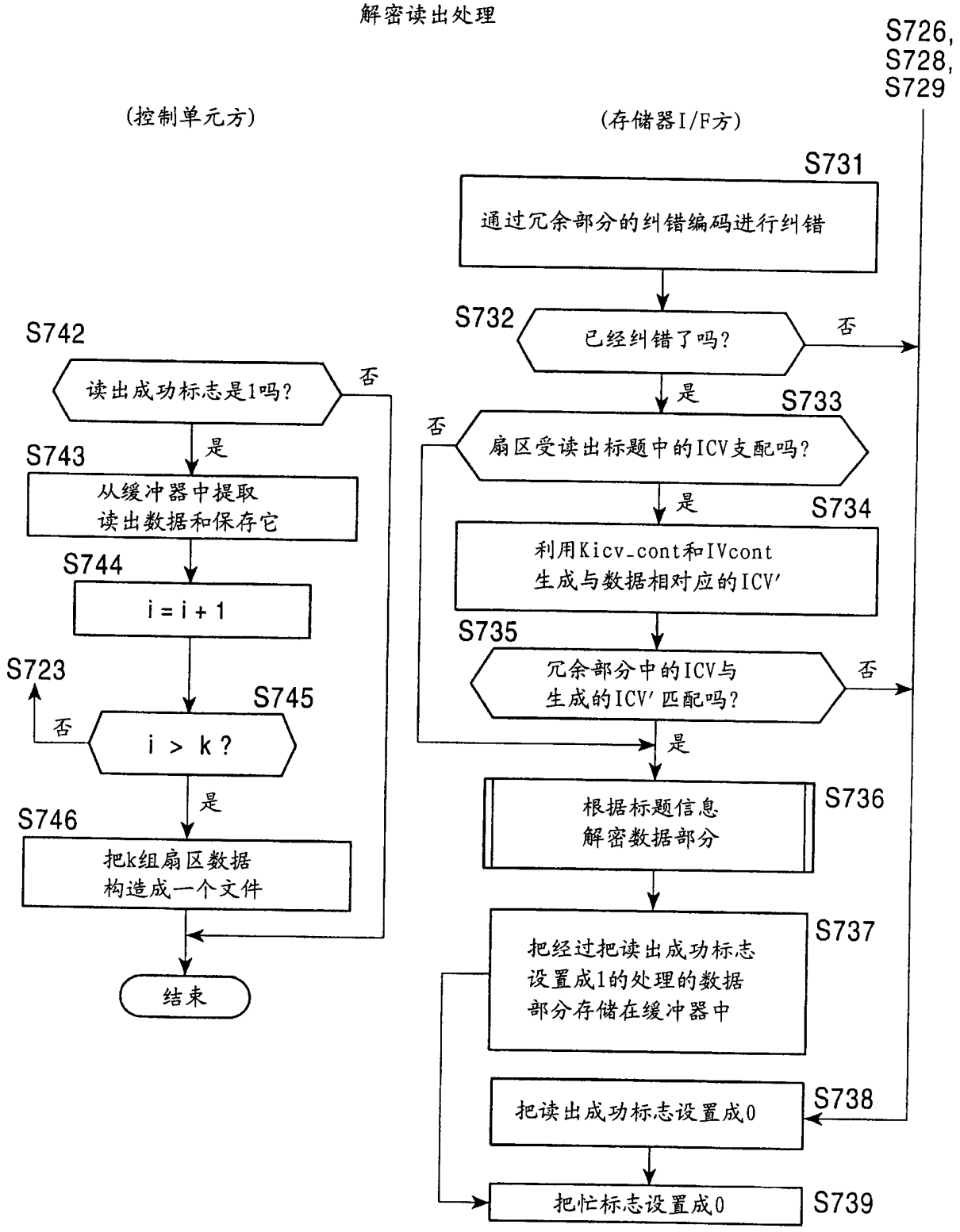

解密读出处理
(控制单元方)
(存储器I/F方)
S726,
S728,
S729
S731
通过冗余部分的纠错编码进行纠错
S732
已经纠错了吗?
否
是
S733
扇区受读出标题中的ICV支配吗?
否
是
S734
利用Kicv_cont和IVcont
生成与数据相对应的ICV′
S735
冗余部分中的ICV与
生成的ICV′匹配吗?
否
是
S736
根据标题信息
解密数据部分
S737
把经过把读出成功标志
设置成1的处理的数据
部分存储在缓冲器中
S738
把读出成功标志设置成0
S739
把忙标志设置成0
S742
读出成功标志是1吗?
否
是
S743
从缓冲器中提取
读出数据和保存它
S744
i = i + 1
S723
否
S745
i > k ?
是
S746
把k组扇区数据
构造成一个文件
结束

图 36-2

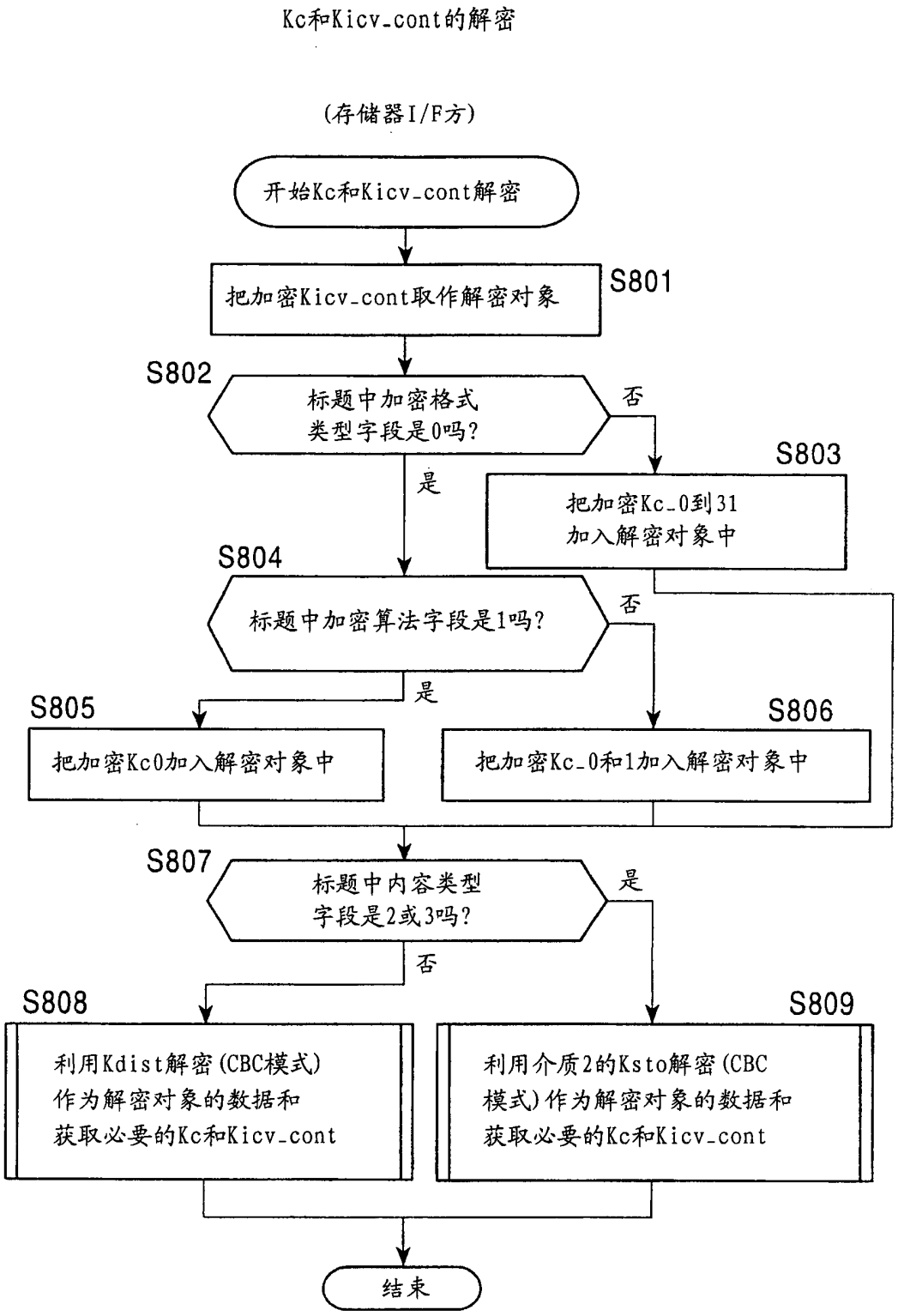

Kc和Kicv_cont的解密
(存储器I/F方)
开始Kc和Kicv_cont解密
把加密Kicv_cont取作解密对象
S801
S802
标题中加密格式
类型字段是0吗?
否
是
S803
把加密Kc_0到31
加入解密对象中
S804
标题中加密算法字段是1吗?
否
是
S805
把加密Kc0加入解密对象中
S806
把加密Kc_0和1加入解密对象中
S807
标题中内容类型
字段是2或3吗?
是
否
S808
利用Kdist解密(CBC模式)
作为解密对象的数据和
获取必要的Kc和Kicv_cont
S809
利用介质2的Ksto解密(CBC
模式)作为解密对象的数据和
获取必要的Kc和Kicv_cont
结束

图 37

利用介质2的Ksto解密要解密的数据

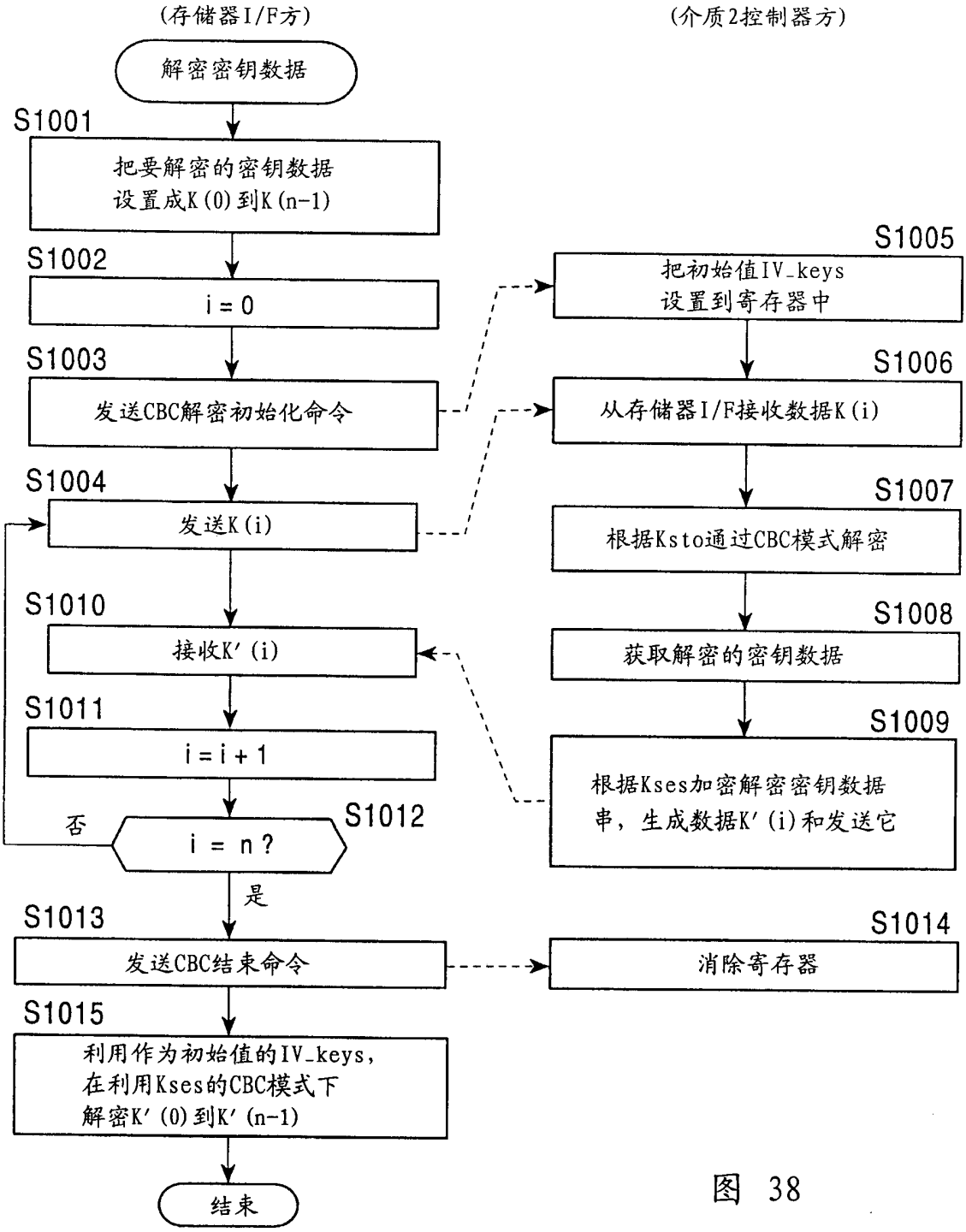


图 38

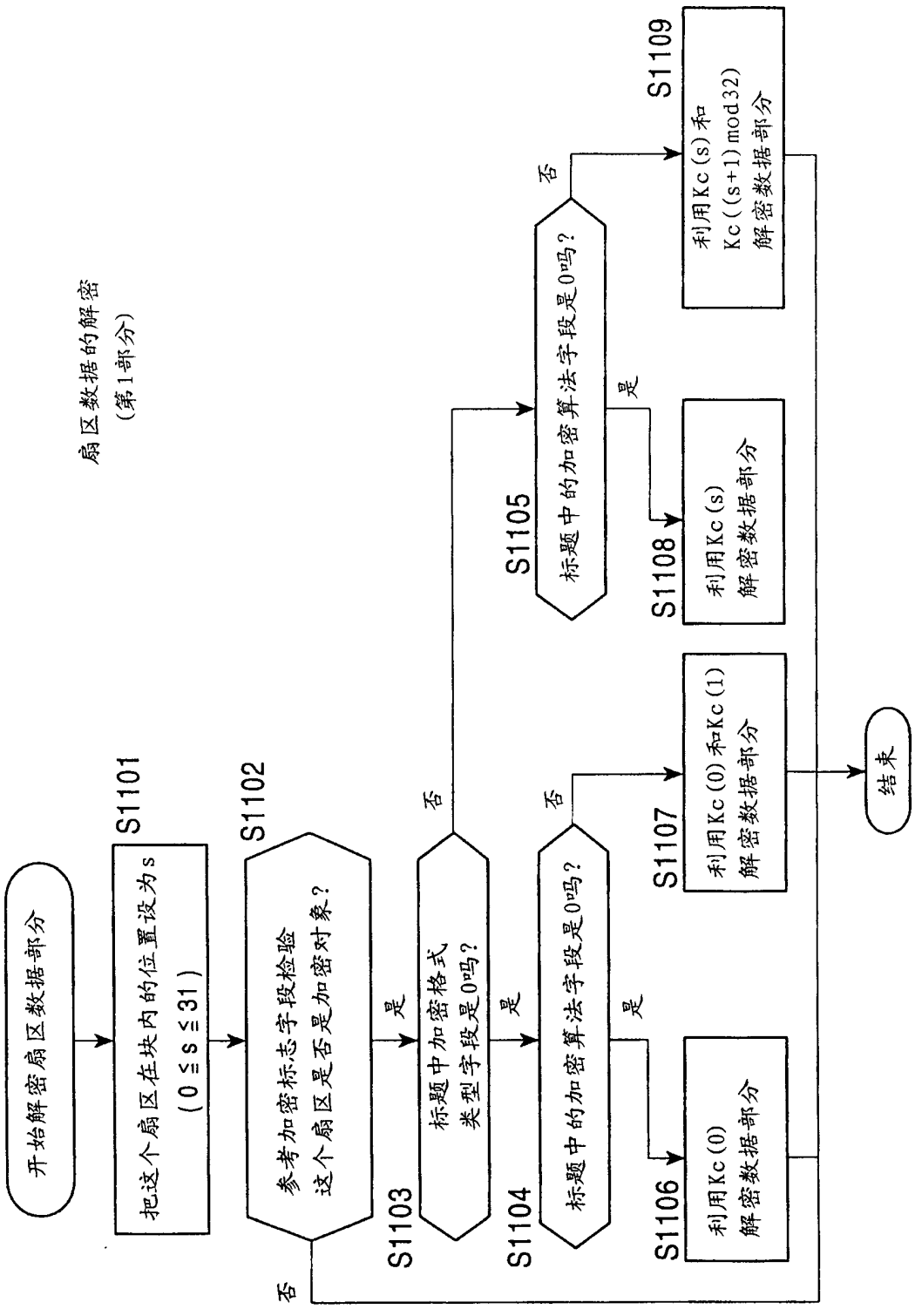

扇区数据的解密
(第1部分)
开始解密扇区数据部分
S1101
把这个扇区在块内的位置设为s
(0≤s≤31)
S1102
参考加密标志字段检验
这个扇区是否是加密对象?
否
是
S1103
标题中加密格式
类型字段是0吗?
否
是
S1104
标题中的加密算法字段是0吗?
否
是
S1105
标题中的加密算法字段是0吗?
否
是
S1106
利用Kc(0)
解密数据部分
S1107
利用Kc(0)和Kc(1)
解密数据部分
S1108
利用Kc(s)
解密数据部分
S1109
利用Kc(s)和
Kc((s+1) mod32)
解密数据部分
结束

图 39

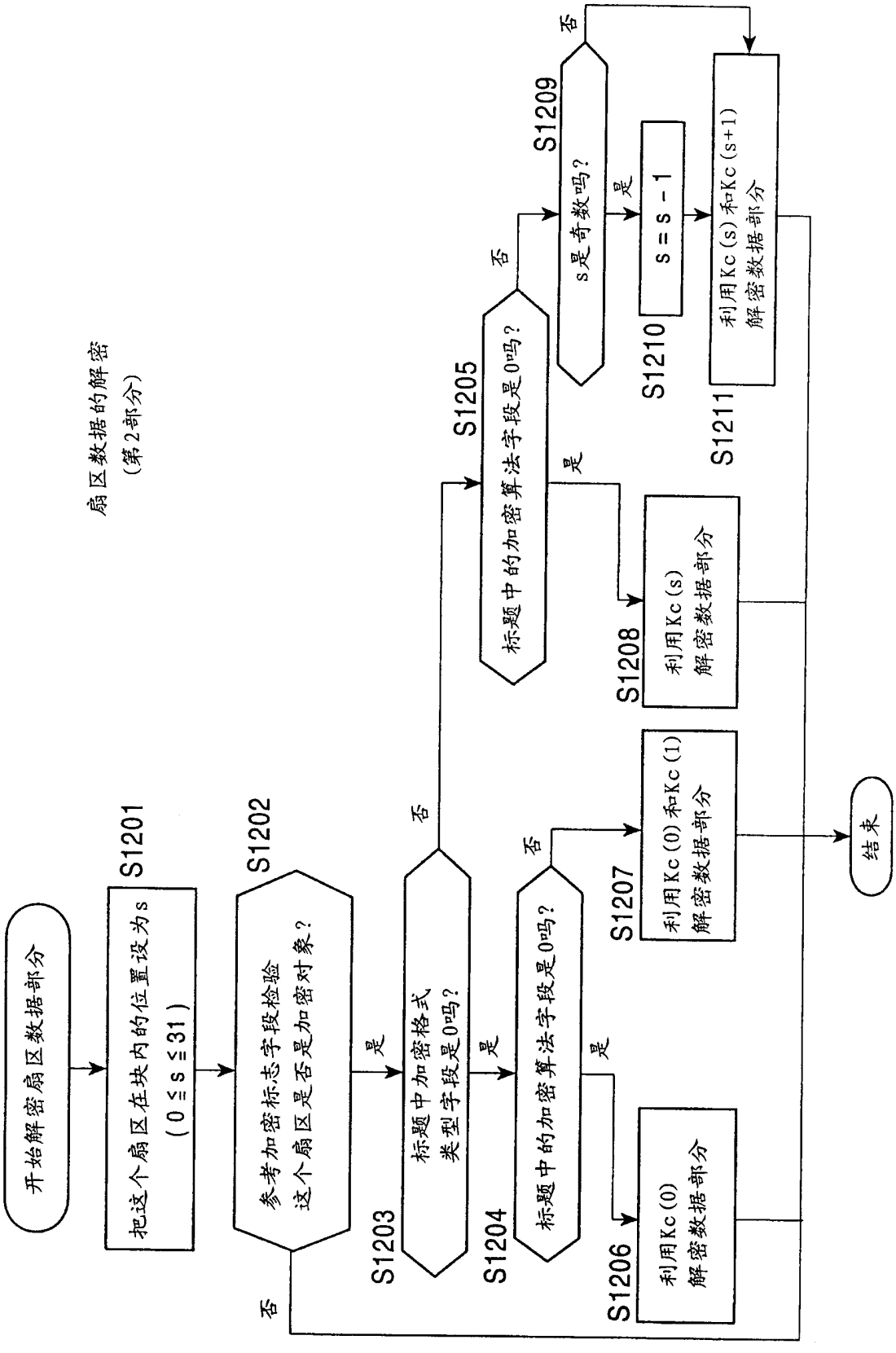

扇区数据的解密
(第2部分)
开始解密扇区数据部分
S1201
把这个扇区在块内的位置设为s
(0≤s≤31)
S1202
参考加密标志字段检验
这个扇区是否是加密对象?
否
是
S1203
标题中加密格式
类型字段是0吗?
否
是
S1204
标题中的加密算法字段是0吗?
否
是
S1205
标题中的加密算法字段是0吗?
否
是
S1206
利用Kc(0)
解密数据部分
S1207
利用Kc(0)和Kc(1)
解密数据部分
S1208
利用Kc(s)
解密数据部分
S1209
s是奇数吗?
否
是
S1210
s=s-1
S1211
利用Kc(s)和Kc(s+1)
解密数据部分
结束

图 40

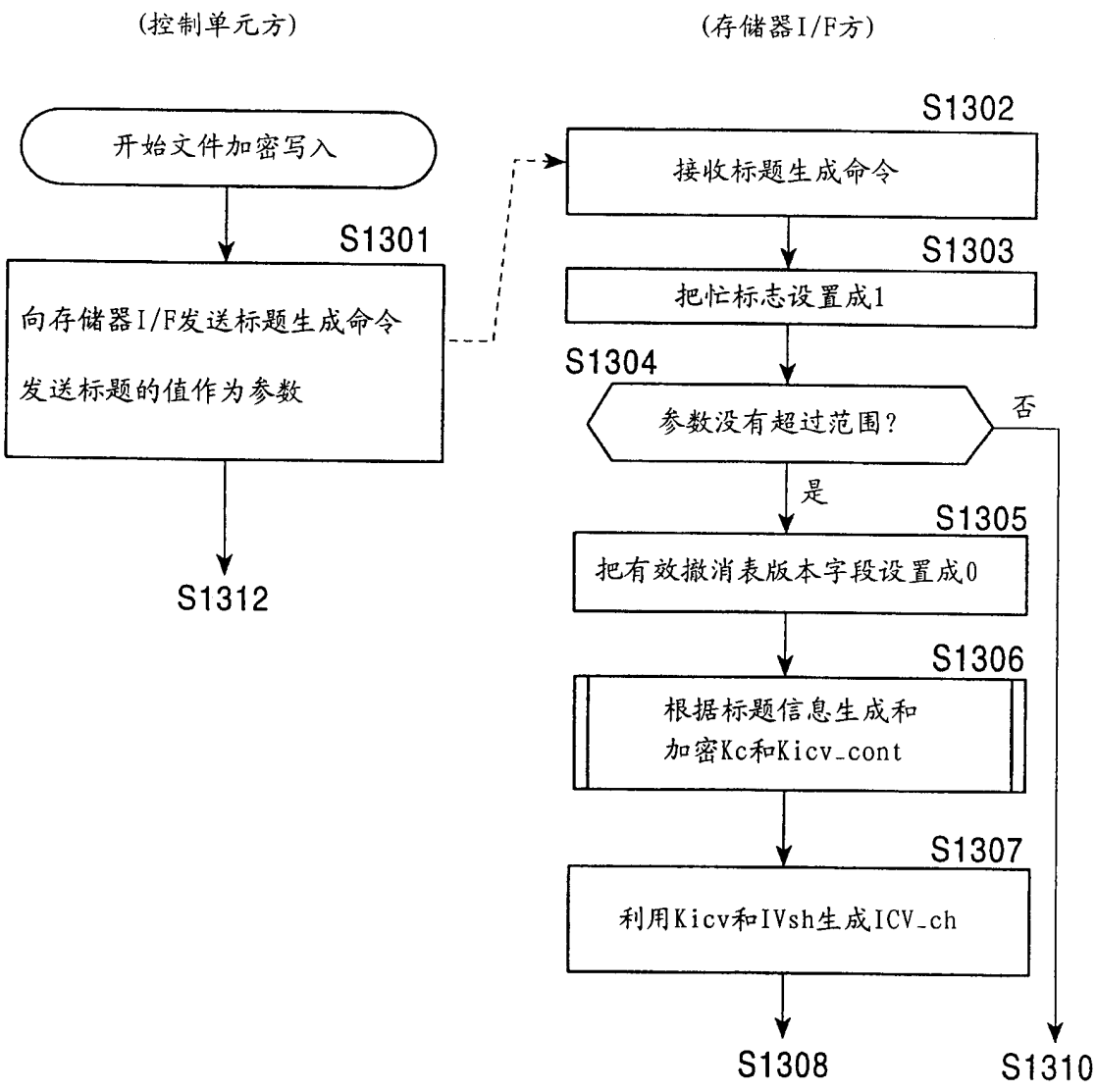

文件加密写入处理
(控制单元方)
(存储器I/F方)
开始文件加密写入
S1301
向存储器I/F发送标题生成命令
发送标题的值作为参数
S1312
S1302
接收标题生成命令
S1303
把忙标志设置成1
S1304
参数没有超过范围?
否
是
S1305
把有效撤消表版本字段设置成0
S1306
根据标题信息生成和
加密Kc和Kicv_cont
S1307
利用Kicv和IVsh生成ICV_ch
S1308
S1310

图 41-1

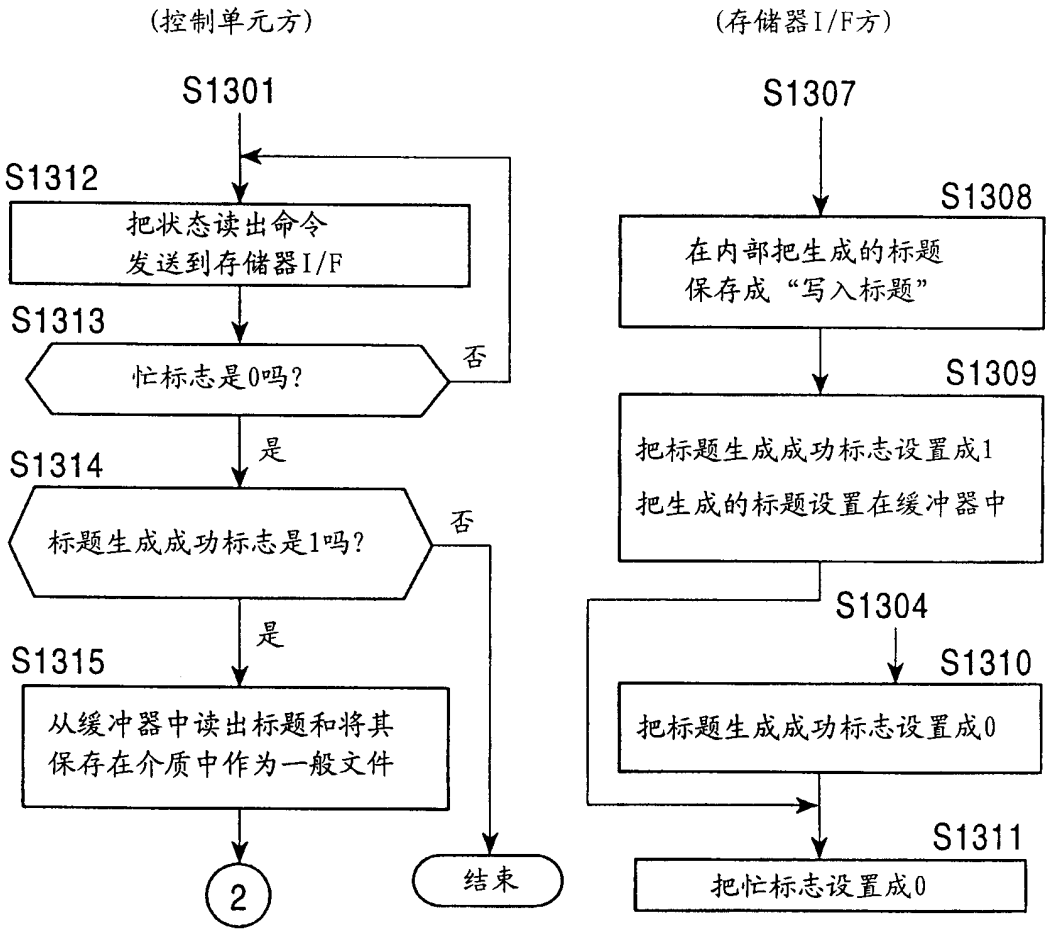

文件加密写入处理
(控制单元方)
(存储器I/F方)
S1301
S1312
把状态读出命令
发送到存储器I/F
S1313
忙标志是0吗?
否
是
S1314
标题生成成功标志是1吗?
否
是
S1315
从缓冲器中读出标题和将其
保存在介质中作为一般文件
2
结束
S1307
S1308
在内部把生成的标题
保存成“写入标题”
S1309
把标题生成成功标志设置成1
把生成的标题设置在缓冲器中
S1304
S1310
把标题生成成功标志设置成0
S1311
把忙标志设置成0

图 41-2

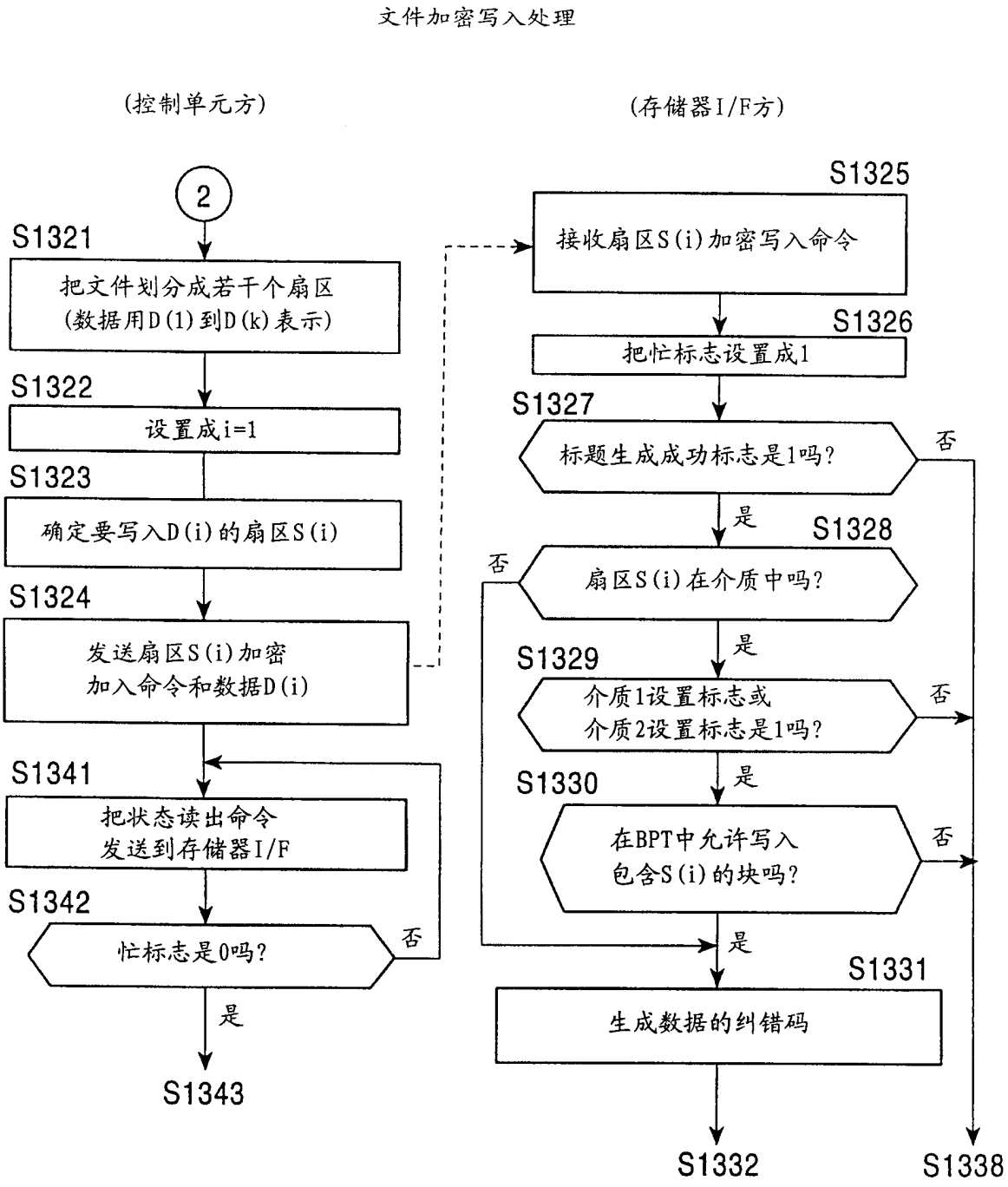

文件加密写入处理
(控制单元方)
(存储器I/F方)
2
S1321
把文件划分成若干个扇区
(数据用D(1)到D(k)表示)
S1322
设置成i=1
S1323
确定要写入D(i)的扇区S(i)
S1324
发送扇区S(i)加密
加入命令和数据D(i)
S1341
把状态读出命令
发送到存储器I/F
S1342
忙标志是0吗?
否
是
S1343
S1325
接收扇区S(i)加密写入命令
S1326
把忙标志设置成1
S1327
标题生成成功标志是1吗?
否
是
S1328
否
扇区S(i)在介质中吗?
是
S1329
介质1设置标志或
介质2设置标志是1吗?
否
是
S1330
在BPT中允许写入
包含S(i)的块吗?
否
是
S1331
生成数据的纠错码
S1332
S1338

图 42-1

文件加密写入处理

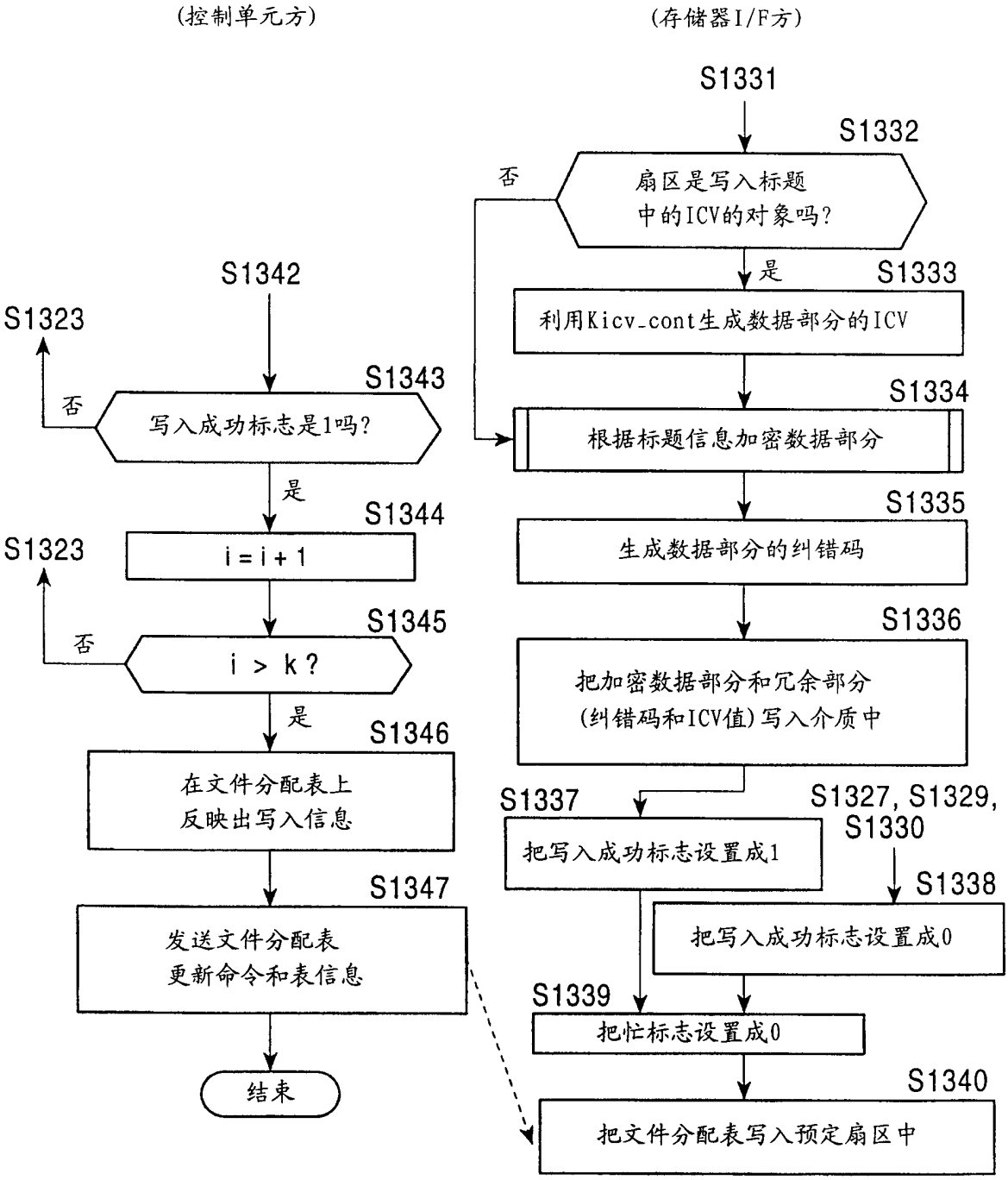


图 42-2

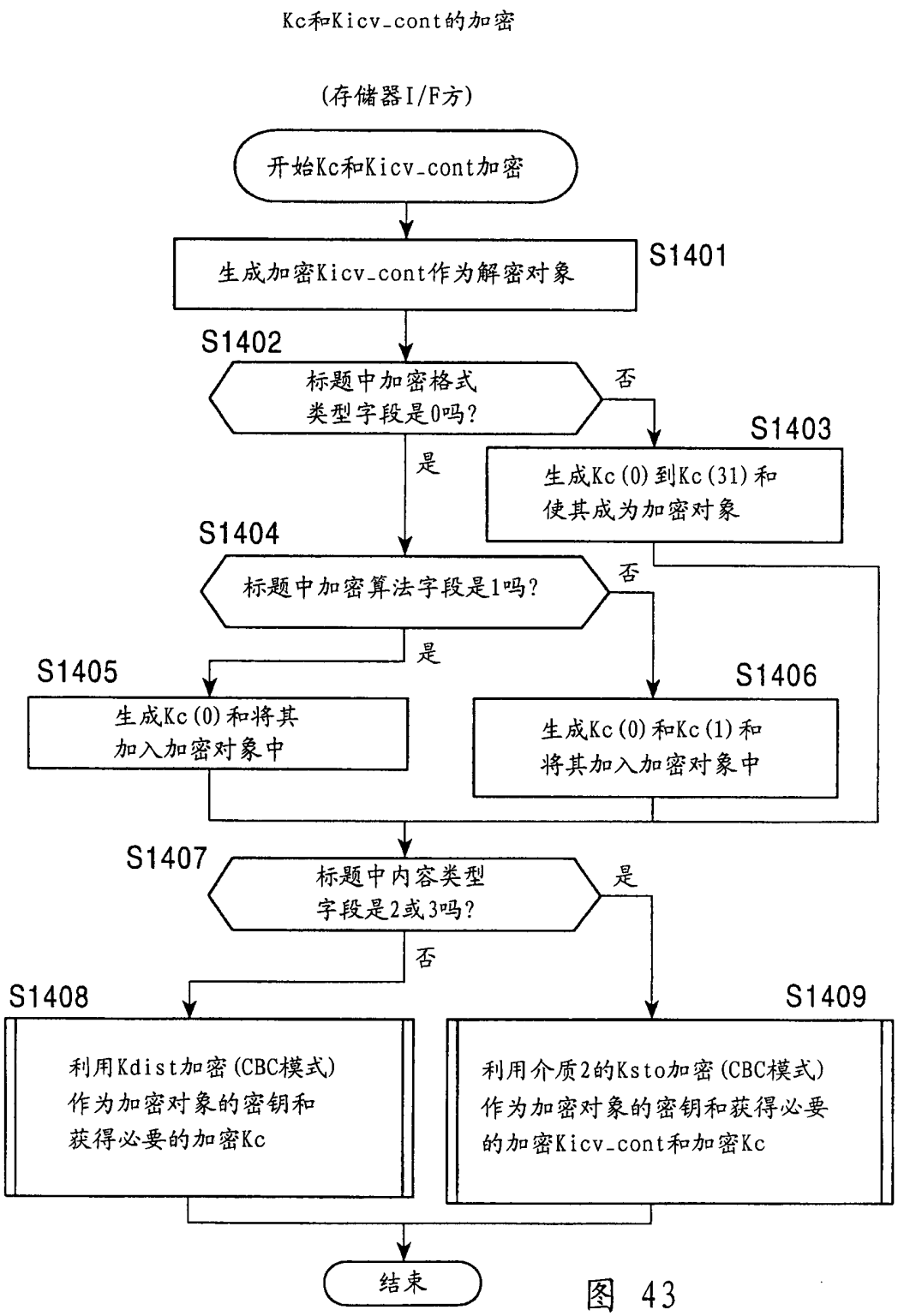

Kc和Kicv_cont的加密
(存储器I/F方)
开始Kc和Kicv_cont加密
生成加密Kicv_cont作为解密对象
S1401
S1402
标题中加密格式
类型字段是0吗?
否
是
S1403
生成Kc(0)到Kc(31)和
使其成为加密对象
S1404
标题中加密算法字段是1吗?
否
是
S1405
生成Kc(0)和将其
加入加密对象中
S1406
生成Kc(0)和Kc(1)和
将其加入加密对象中
S1407
标题中内容类型
字段是2或3吗?
是
否
S1408
利用Kdist加密(CBC模式)
作为加密对象的密钥和
获得必要的加密Kc
S1409
利用介质2的Ksto加密(CBC模式)
作为加密对象的密钥和获得必要
的加密Kicv_cont和加密Kc
结束

图 43

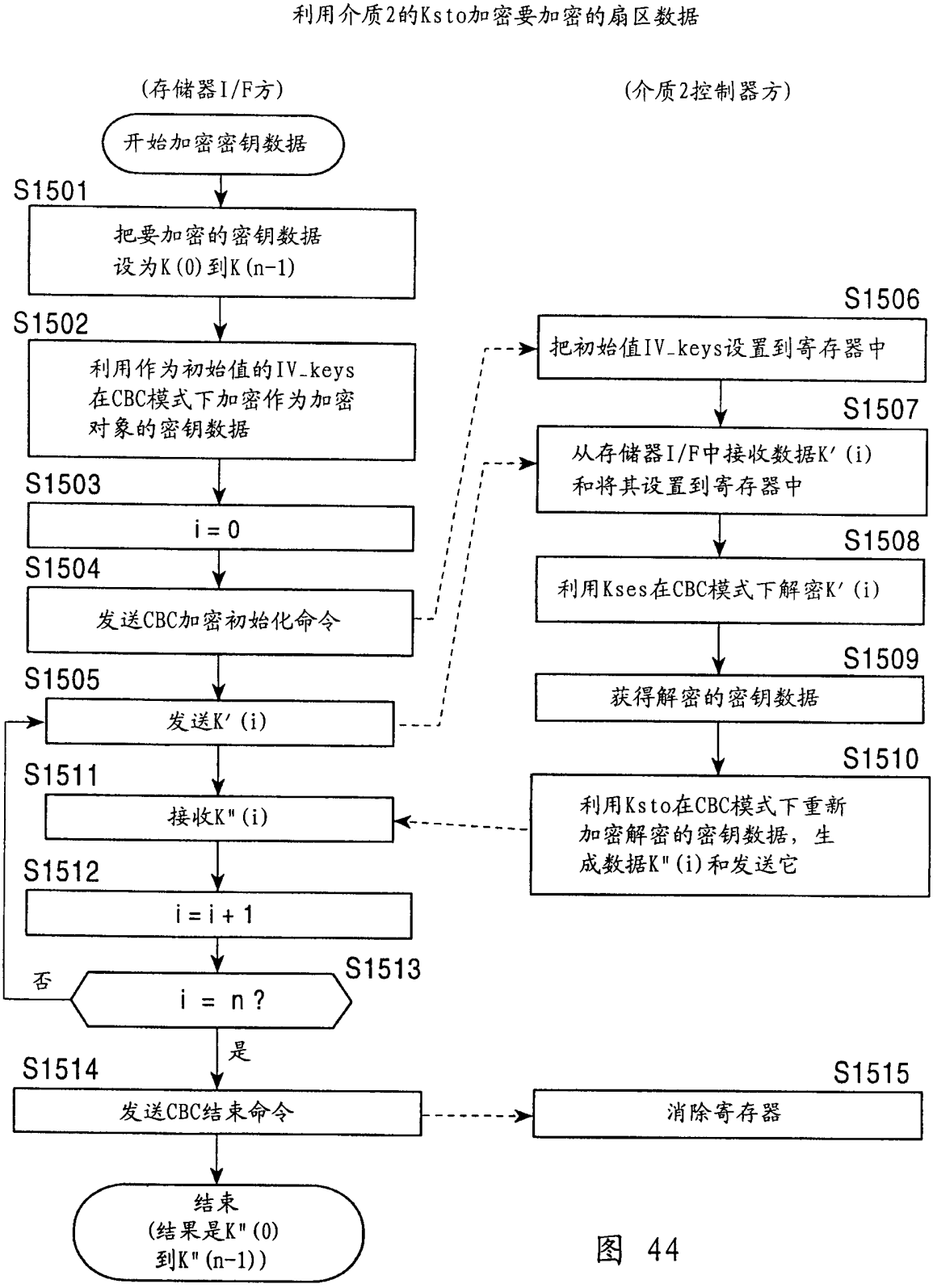

利用介质2的Ksto加密要加密的扇区数据
(存储器I/F方)
(介质2控制器方)
开始加密密钥数据
S1501
把要加密的密钥数据
设为K(0)到K(n-1)
S1502
利用作为初始值的IV_keys
在CBC模式下加密作为加密
对象的密钥数据
S1503
i = 0
S1504
发送CBC加密初始化命令
S1505
发送K′(i)
S1511
接收K"(i)
S1512
i = i + 1
否
S1513
i = n ?
是
S1514
发送CBC结束命令
结束
(结果是K"(0)
到K"(n-1))
S1506
把初始值IV_keys设置到寄存器中
S1507
从存储器I/F中接收数据K′(i)
和将其设置到寄存器中
S1508
利用Kses在CBC模式下解密K′(i)
S1509
获得解密的密钥数据
S1510
利用Ksto在CBC模式下重新
加密解密的密钥数据，生
成数据K"(i)和发送它
S1515
消除寄存器

图 44

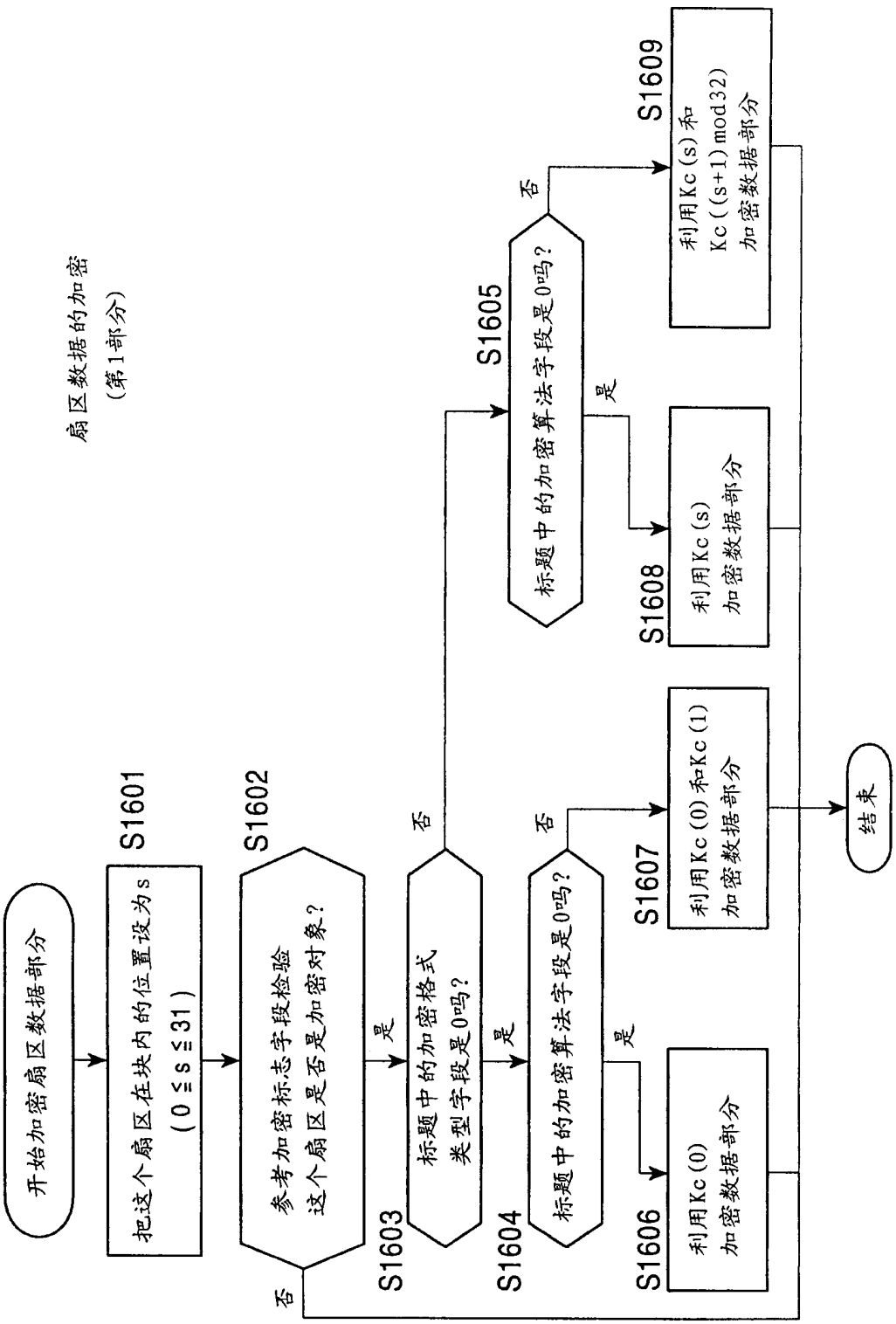

扇区数据的加密
(第1部分)
开始加密扇区数据部分
S1601
把这个扇区在块内的位置设为s
(0≦s≦31)
S1602
参考加密标志字段检验
这个扇区是否是加密对象?
否
是
S1603
标题中的加密格式
类型字段是0吗?
否
是
S1604
标题中的加密算法字段是0吗?
否
是
S1605
标题中的加密算法字段是0吗?
否
是
S1606
利用Kc(0)
加密数据部分
S1607
利用Kc(0)和Kc(1)
加密数据部分
S1608
利用Kc(s)
加密数据部分
S1609
利用Kc(s)和
Kc((s+1) mod32)
加密数据部分
结束

图 45

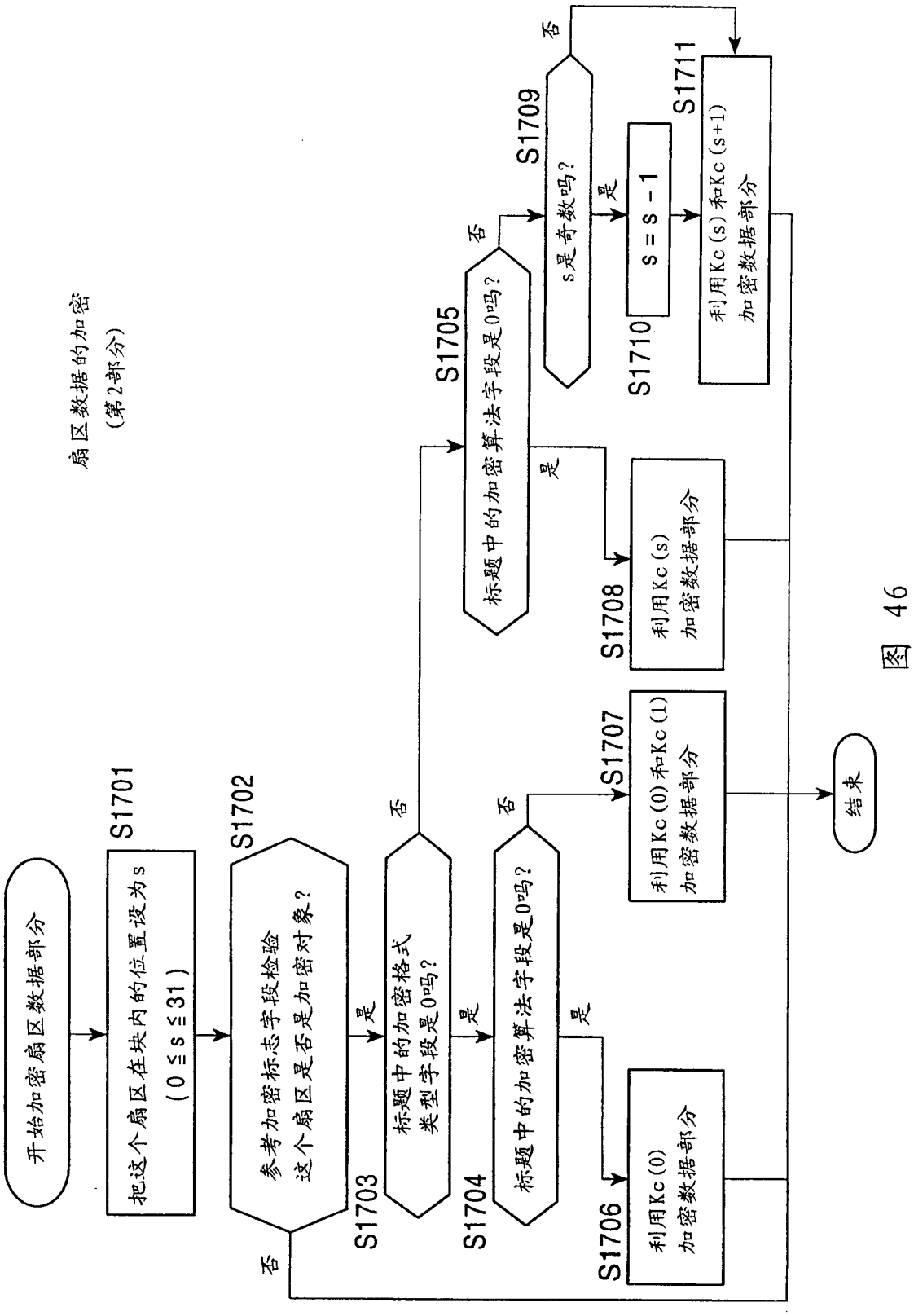

扇区数据的加密
(第2部分)
开始加密扇区数据部分
S1701
把这个扇区在块内的位置设为s
(0≤s≤31)
S1702
参考加密标志字段检验
这个扇区是否是加密对象?
否
是
S1703
标题中的加密格式
类型字段是0吗?
否
是
S1704
标题中的加密算法字段是0吗?
否
是
S1705
标题中的加密算法字段是0吗?
否
是
S1706
利用Kc(0)
加密数据部分
S1707
利用Kc(0)和Kc(1)
加密数据部分
S1708
利用Kc(s)
加密数据部分
S1709
s是奇数吗?
否
是
S1710
s=s-1
S1711
利用Kc(s)和Kc(s+1)
加密数据部分
结束

图 46

撤消表的更新

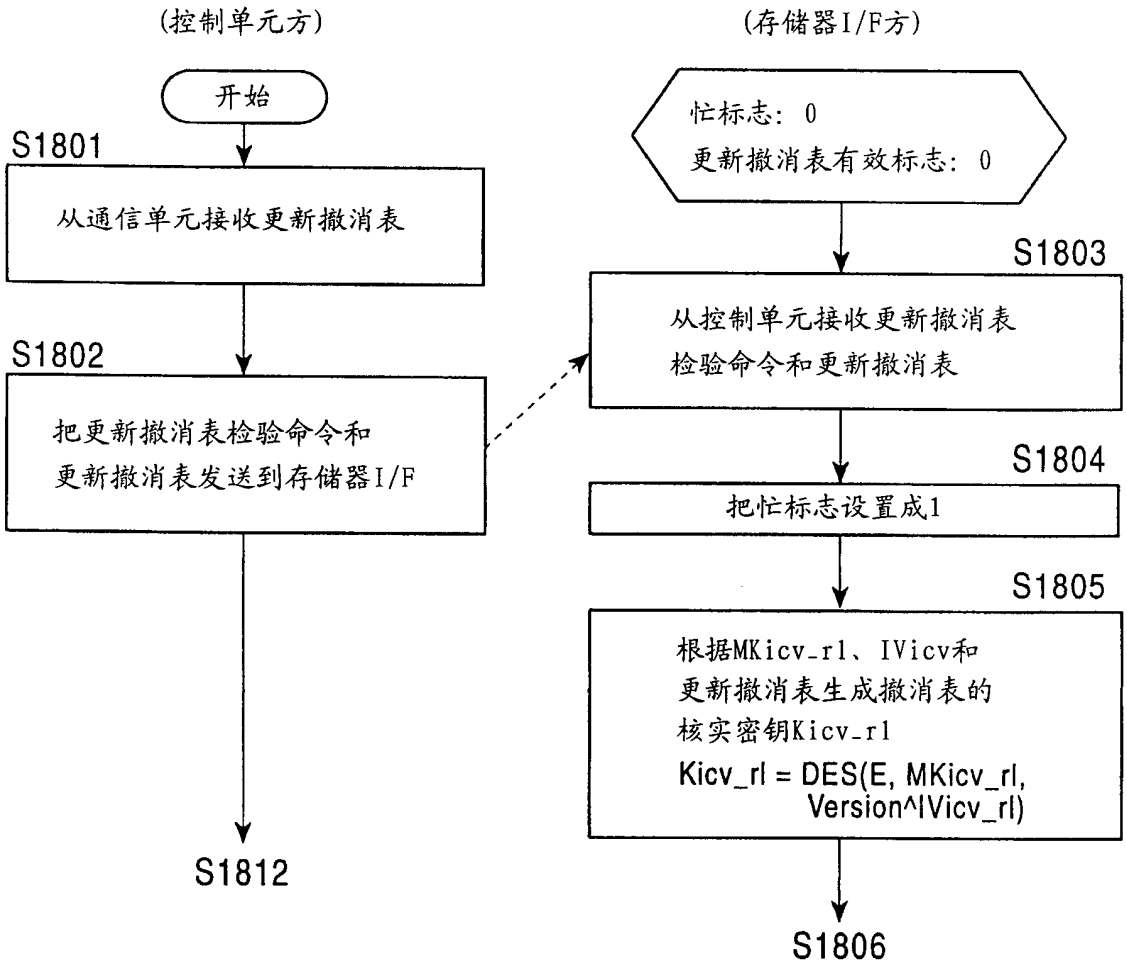

(控制单元方)
(存储器I/F方)
开始
S1801
从通信单元接收更新撤消表
S1802
把更新撤消表检验命令和
更新撤消表发送到存储器I/F
S1812
忙标志: 0
更新撤消表有效标志: 0
S1803
从控制单元接收更新撤消表
检验命令和更新撤消表
S1804
把忙标志设置成1
S1805
根据MKicv_rl、IVicv和
更新撤消表生成撤消表的
核实密钥Kicv_rl
Kicv_rl = DES(E, MKicv_rl,
Version^IVicv_rl)
S1806

图 47-1

撤消表的更新

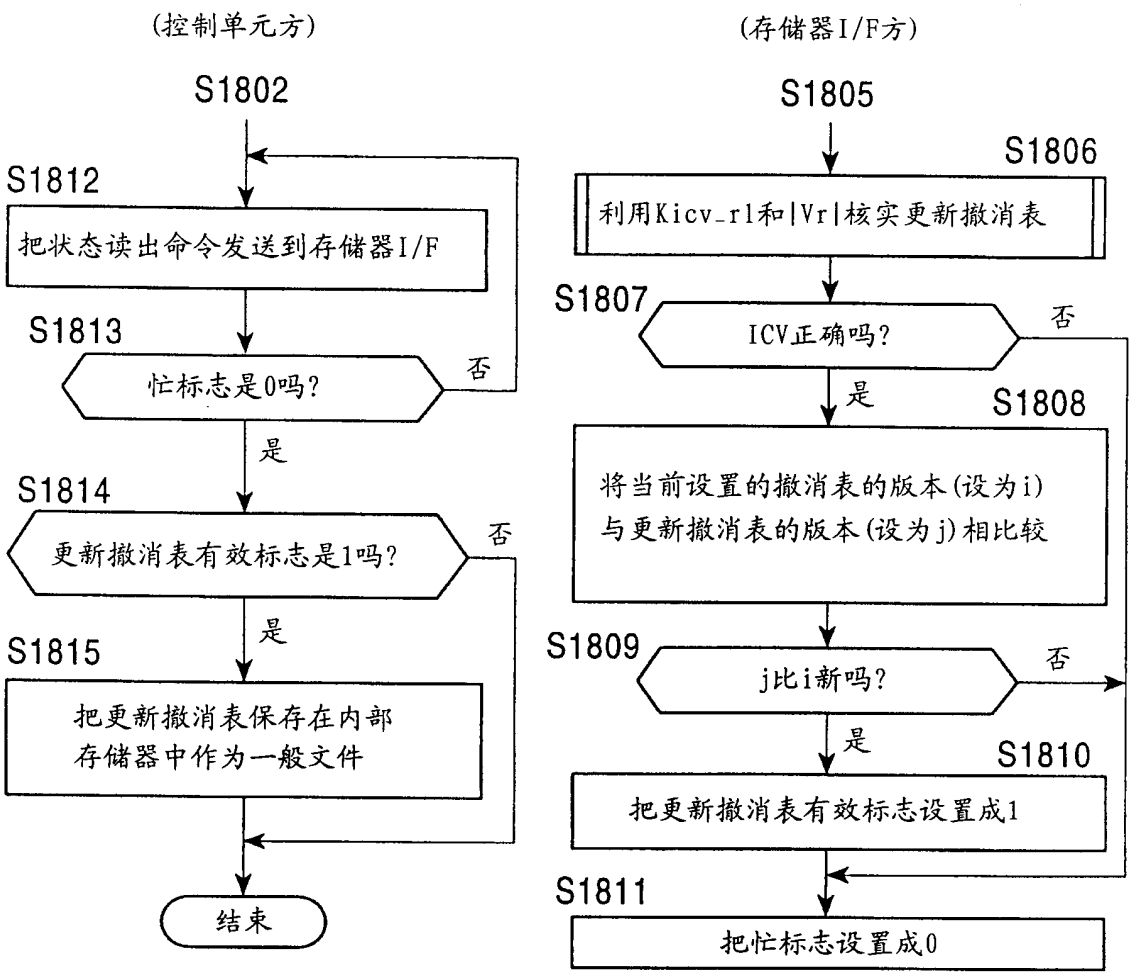

(控制单元方)
S1802
S1812
把状态读出命令发送到存储器I/F
S1813
忙标志是0吗?
否
是
S1814
更新撤消表有效标志是1吗?
否
是
S1815
把更新撤消表保存在内部
存储器中作为一般文件
结束
(存储器I/F方)
S1805
S1806
利用Kicv_rl和|Vr|核实更新撤消表
S1807
ICV正确吗?
否
是
S1808
将当前设置的撤消表的版本(设为i)
与更新撤消表的版本(设为j)相比较
S1809
j比i新吗?
否
是
S1810
把更新撤消表有效标志设置成1
S1811
把忙标志设置成0

图 47-2