(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101025977 B
(45)授权公告日 2012.09.19

(21)申请号 200710002843.5
(22)申请日 2007.02.06
(30)优先权数据
2006-028338 2006.02.06 JP
(73)专利权人 索尼株式会社
地址 日本东京都
(72)发明人 高岛芳和
(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
代理人 刘新宇 权鲜枝
(51)Int.Cl.
G11B 20/00(2006.01)
(56)对比文件
US 2004/0133794 A1,2004.07.08, 全文.
JP 特开2005-354121 A,2005.12.22, 全文.
WO 2005/008385 A2,2005.01.27, 全文.
JP 特开2004-260533 A,2004.09.16, 全文.
审查员 任温馨

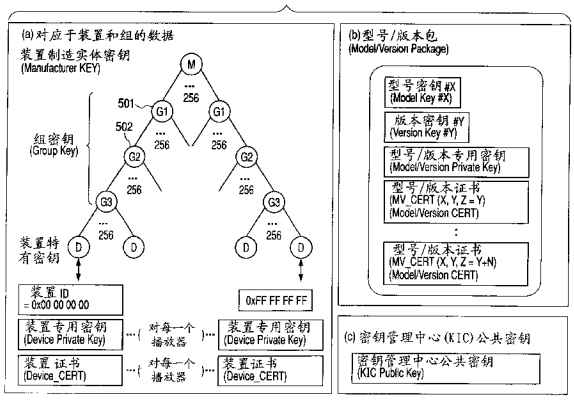
权利要求书 5 页 说明书 35 页 附图 27 页

(54)发明名称

信息处理设备及方法和信息记录介质制造设备及方法

(57)摘要

本发明涉及一种信息处理设备及方法和信息记录介质制造设备及方法。所述信息处理设备包括:数据处理单元,其获取包含记录在信息记录介质中的数据处理程序的内容代码并根据内容代码执行数据处理;以及存储器,其存储包含信息处理设备的设备标识符的设备证书。数据处理单元被配置为根据包含在内容代码中的用于设备检查处理的代码应用存储在存储器中的设备证书执行设备检查处理,在设备检查处理之后获取记录在设备证书中的设备标识符,应用对应于获得的设备标识符的内容代码执行数据处理。



CN 101025977 B

1. 一种信息处理设备，包括：

数据处理单元，其获取包含记录在信息记录介质中的数据处理程序的内容代码，根据所述内容代码执行数据处理；以及

存储器，其存储包含所述信息处理设备的设备标识符的设备证书，

其中，所述数据处理单元被配置为根据包含在所述内容代码中的用于设备检查处理的代码应用存储在所述存储器中的所述设备证书执行设备检查处理，在所述设备检查处理之后获取记录在所述设备证书中的所述设备标识符，应用对应于所获得的设备标识符的内容代码执行数据处理。

2. 根据权利要求 1 所述的信息处理设备，其特征在于，

所述设备证书是存储有信息处理设备特有的装置标识符和装置专用密钥的装置证书，或者是存储有对应于信息处理设备的型号或版本的型号标识符或版本标识符和型号 / 版本公共密钥的型号 / 版本证书，

所述数据处理单元被配置为应用所述装置证书和所述型号 / 版本证书中的至少一个来执行设备检查处理，获取记录在所述装置证书中的装置标识符与记录在所述型号 / 版本证书中的型号标识符 / 版本标识符中的任意一个，应用对应于所获得的标识符的内容代码执行数据处理。

3. 根据权利要求 1 所述的信息处理设备，其特征在于，

所述数据处理单元被配置为通过验证在所述设备证书中设置的签名的处理来检查所述设备证书的有效性，通过使用存储在所述信息处理设备的所述存储器中的专用密钥来产生新的签名数据，通过使用存储在所述设备证书中的公共密钥来验证所产生的签名数据，执行将所述签名验证成功判断为所述设备检查成功的设备检查处理。

4. 根据权利要求 1 所述的信息处理设备，其特征在于，还包括：

存储器，其存储在具有分层结构的密钥树中与作为对应于所述信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从所述叶片到顶层节点的路径上的节点相对应地设置的组密钥、以及与所述顶层节点相对应地设置的装置制造实体密钥作为对应于装置和组的数据，存储与所述信息处理设备的型号 / 版本相对应的型号密钥 / 版本密钥作为型号 / 版本包，并存储密钥管理中心公共密钥，

其中，所述数据处理单元被配置为应用所述密钥管理中心公共密钥执行验证所述内容代码的签名的处理，在应用所述内容代码的数据处理中应用所述装置特有密钥、所述组密钥、所述装置制造实体密钥、所述型号密钥和所述版本密钥中的任意一个执行解密包含在所述内容代码中的数据的处理。

5. 根据权利要求 4 所述的信息处理设备，其特征在于，

所述数据处理单元被配置为从存储在所述信息记录介质中的数据中获取在所述内容代码的解密中应用的密钥指定信息和表示在所述内容代码中设置的加密数据的位置的加密数据位置指定信息，根据获得的信息选择要应用的密钥，根据所述加密数据位置指定信息指定要解密的数据，应用所选择的密钥执行解密处理。

6. 根据权利要求 4 所述的信息处理设备，其特征在于，

所述内容代码具有以作为包含在所述内容代码中的数据的大小为 2MB 的块为单位设置签名的数据结构，

所述数据处理单元被配置为以大小为 2MB 的所述块为单位执行验证所述内容代码的签名的处理。

7. 根据权利要求 4 所述的信息处理设备，其特征在于，

在存储器中存储与对应于信息处理设备的制造商、组件的制造商或组装者的多个不同的装置制造实体相对应的独立密钥集，

所述数据处理单元被配置为在进行解密内容代码的处理时，从对应于与要执行的内容代码相对应地选择的装置制造实体的密钥集中选择密钥，从而执行应用所选择的密钥解密包含在所述内容代码中的数据的处理。

8. 根据权利要求 1 所述的信息处理设备，其特征在于，

所述数据处理单元被配置为至少执行应用包含在所述内容代码中的安全检查代码的安全检查处理和应用包含在所述内容代码中的数据转换表的内容形成数据的数据转换处理中的一个，作为在所述设备检查处理之后执行的应用所述内容代码的数据处理。

9. 根据权利要求 1 所述的信息处理设备，其特征在于，

所述信息处理设备被配置为将存储有与所述信息处理设备的型号 / 版本相对应的型号 / 版本公共密钥的型号 / 版本证书存储在存储器中，

所述数据处理单元被配置为通过检查记录在所述型号 / 版本证书中的证书更新信息来确定所述内容代码的应用状态。

10. 一种信息记录介质制造设备，包括 ：

内容文件产生装置，用于产生存储记录在信息记录介质中的内容数据的内容文件 ；

内容代码文件产生装置，用于产生存储包含当使用内容时所执行的数据处理程序的内容代码的内容代码文件 ；以及

记录装置，用于在信息记录介质中记录所述内容文件产生装置产生的内容文件和所述内容代码文件产生装置产生的内容代码文件，

其中，所述内容代码文件产生装置被配置为产生存储有使得执行应用存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的用于设备检查处理的代码的内容代码文件，和产生存储有根据所述设备检查处理检查后的设备标识符选择并执行的安全检查代码的内容代码文件。

11. 根据权利要求 10 所述的信息记录介质制造设备，其特征在于，

所述内容代码文件产生装置被配置为产生存储有在根据所述设备检查处理检查后的设备标识符选择并执行的内容的数据转换处理中所应用的数据转换表的内容代码文件。

12. 根据权利要求 10 所述的信息记录介质制造设备，其特征在于，

所述内容代码文件产生装置被配置为产生存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件。

13. 根据权利要求 12 所述的信息记录介质制造设备，其特征在于，

所述加密密钥对应于在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从所述叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与所述顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应的型号密钥和与信息处理设备的版本相对应的版本密钥中的任意一个。

14. 根据权利要求 12 所述的信息记录介质制造设备，其特征在于，

所述内容代码文件产生装置被配置为执行如下处理：产生作为要在信息记录介质中记录的信息的加密数据部分和包含密钥指定信息的内容代码加密信息，作为与存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件相对应的信息。

15. 一种信息处理方法，其应用信息处理设备中的信息记录介质的记录数据执行数据处理，所述信息处理方法包括如下步骤：

在数据处理单元中获取包含记录在所述信息记录介质中的数据处理程序的内容代码；

在所述数据处理单元中根据包含在所述内容代码中的用于设备检查处理的代码应用存储在存储器中的设备证书执行设备检查处理；以及

在所述数据处理单元中执行内容代码处理，在所述内容代码处理中，获取记录在所述设备证书中的设备标识符，选择对应于获得的设备标识符的内容代码，应用所选择的内容代码执行数据处理。

16. 根据权利要求 15 所述的信息处理方法，其特征在于，

所述设备证书是存储有信息处理设备特有的装置标识符和装置专用密钥的装置证书，或者是存储有对应于信息处理设备的型号或版本的型号标识符或版本标识符和型号 / 版本公共密钥的型号 / 版本证书，

在执行所述设备检查处理中，执行应用所述装置证书和所述型号 / 版本证书中的至少一个的设备检查处理，获取记录在所述装置证书中的装置标识符与记录在所述型号 / 版本证书中的型号标识符 / 版本标识符中的任意一个，

在执行所述内容代码处理中，执行应用对应于所获得的标识符的内容代码的数据处理。

17. 根据权利要求 15 所述的信息处理方法，其特征在于，

在执行所述设备检查处理中，通过验证在所述设备证书中设置的签名的处理来检查设备证书的有效性，使用存储在所述信息处理设备的存储器中的专用密钥来产生新的签名数据，使用存储在所述设备证书中的公共密钥来验证产生的签名数据，执行将所述签名验证成功判断为所述设备检查成功的设备检查处理。

18. 根据权利要求 15 所述的信息处理方法，其特征在于，

所述信息处理设备包括：

存储器，其存储在具有分层结构的密钥树中与作为对应于所述信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从所述叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与所述顶层节点相对应地设置的装置制造实体密钥作为对应于装置和组的数据，存储与信息处理设备的型号 / 版本相对应的型号密钥 / 版本密钥作为型号 / 版本包，并存储密钥管理中心公共密钥，

所述数据处理单元应用所述密钥管理中心公共密钥执行验证所述内容代码的签名的处理，在执行所述内容代码处理中应用所述装置特有密钥、所述组密钥、所述装置制造实体密钥、所述型号密钥和所述版本密钥中的任意一个执行解密包含在内容代码中的数据的处理。

19. 根据权利要求 18 所述的信息处理方法，其特征在于，

在执行所述内容代码处理中，从存储在所述信息记录介质中的数据中获取在所述内容代码的解密中应用的密钥指定信息和表示在所述内容代码中设置的加密数据的位置的加密数据位置指定信息，根据获得的信息选择要应用的密钥，根据所述加密数据位置指定信息指定要解密的数据，应用所选择的密钥执行解密处理。

20. 根据权利要求 18 所述的信息处理方法，其特征在于，

所述内容代码具有以作为包含在所述内容代码中的数据的大小为 2MB 的块为单位设置签名的数据结构，

在所述数据处理单元中以大小为 2MB 的所述块为单位执行验证所述内容代码的签名的处理。

21. 根据权利要求 18 所述的信息处理方法，其特征在于，

在执行所述内容代码处理中，在进行解密内容代码的处理时，从对应于与要执行的内容代码相对应地选择的装置制造实体的密钥集中选择密钥，从而执行应用所选择的密钥解密包含在所述内容代码中的数据的处理。

22. 根据权利要求 15 所述的信息处理方法，其特征在于，

在执行所述内容代码处理中，所述数据处理单元执行应用包含在所述内容代码中的安全检查代码的安全检查处理和应用包含在所述内容代码中的数据转换表的内容形成数据的数据转换处理中的至少一个，作为在所述设备检查处理之后执行的应用内容代码的数据处理。

23. 根据权利要求 15 所述的信息处理方法，其特征在于，还包括如下步骤：

在所述数据处理单元中执行通过检查记录在所述型号 / 版本证书中的证书更新信息来确定所述内容代码的应用状态的处理，

所述信息处理设备被配置为将存储有对应于所述信息处理设备的型号 / 版本的型号 / 版本公共密钥的型号 / 版本证书存储在存储器中。

24. 一种信息记录介质制造设备的信息记录介质制造方法，包括如下步骤：

产生存储记录在信息记录介质中的内容数据的内容文件；

产生存储包含当使用内容时所执行的数据处理程序的内容代码的内容代码文件；以及

在信息记录介质中记录在产生内容文件中产生的内容文件和在产生内容代码文件中产生的内容代码文件，

其中，在产生内容代码文件中，产生存储有使得执行应用存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的用于设备检查处理后的代码的内容代码文件，和存储有根据所述设备检查处理检查后的设备标识符选择并执行的安全检查代码的内容代码文件。

25. 根据权利要求 24 所述的信息记录介质制造方法，其特征在于，

在产生内容代码文件中，产生存储有在根据所述设备检查处理检查后的设备标识符选择并执行的内容的数据转换处理中应用的数据转换表的内容代码文件。

26. 根据权利要求 24 所述的信息记录介质制造方法，其特征在于，

在产生内容代码文件中，产生存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件。

27. 根据权利要求 26 所述的信息记录介质制造方法，其特征在于，

所述加密密钥对应于在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从所述叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与所述顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应的型号密钥和与信息处理设备的版本相对应的版本密钥中的任意一个。

28. 根据权利要求 26 所述的信息记录介质制造方法，其特征在于，

在产生内容代码文件中，执行如下处理：产生作为要在信息记录介质中记录的信息的加密数据部分和包含密钥指定信息的内容代码加密信息，作为与存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件相对应的信息。

29. 一种信息处理设备，包括：

第一存储器，其存储包含每一个信息处理设备特有的数据的数据；以及

第二存储器，其存储与信息处理设备的共有型号和版本相对应的共有数据，

其中，所述包含每一个信息处理设备特有的数据的数据包括包含设备标识符的设备证书、对应于装置制造实体的密钥、将设备划分为组时所设定的预定组共有的组密钥、以及每一个设备特有的密钥，

所述与共有型号和版本相对应的共有数据包括型号特有的密钥、版本特有的密钥和包含型号和版本的标识符的设备证书。

30. 根据权利要求 29 所述的信息处理设备，其特征在于，

根据获得的程序，执行基于所述设备证书的第一签名验证，然后对应于所述第一签名验证的结果进一步执行使用设备特有的密钥的签名验证，执行基于包含型号和版本标识符的所述设备证书的第二签名验证，然后对应于所述第二签名验证的结果进一步执行使用型号特有的密钥或版本特有的密钥的签名验证。

31. 一种信息记录介质制造设备，包括：

内容文件产生单元，用于产生存储记录在信息记录介质中的内容数据的内容文件；

内容代码文件产生单元，用于产生存储包含当使用内容时所执行的数据处理程序的内容代码的内容代码文件；以及

记录单元，用于在信息记录介质中记录所述内容文件产生单元产生的内容文件和所述内容代码文件产生单元产生的内容代码文件，

其中，所述内容代码文件产生单元被配置为产生存储有使得执行应用存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的用于设备检查处理的代码的内容代码文件，和产生存储有根据所述设备检查处理检查后的设备标识符选择并执行的安全检查代码的内容代码文件。

信息处理设备及方法和信息记录介质制造设备及方法

技术领域

[0001] 本发明涉及一种信息处理设备、信息记录介质制造设备、信息记录介质、信息处理方法、信息记录介质制造方法及计算机程序。更具体地，本发明涉及一种信息处理设备、信息记录介质制造设备、信息记录介质、信息处理方法、信息记录介质制造方法及计算机程序，其用于在使用与内容一起记录在信息记录介质中、当使用内容时所执行的内容代码(content code)进行处理时确定对应于信息处理设备的装置、型号或版本，根据所确定的信息选择并执行对应于该信息处理设备的内容代码。

[0002] 背景技术

[0003] 可以将音乐等音频数据、电影等图像数据、游戏程序或各种应用程序即各种软件数据（下文中总称为“内容”）作为数字数据存储在例如使用蓝色激光的蓝光盘(Blu-ray disc，注册商标)、DVD(数字通用盘，digital versatile disc)，MD(小型盘，mini disc)或CD(光盘，compact disc)等记录介质中。尤其是，使用蓝色激光的蓝光盘（注册商标）是高密度可记录盘，可以将大量视频内容等作为高分辨率的数据记录在蓝光盘中。

[0004] 将数字内容存储在这些不同的信息记录介质（存储介质）中，提供给用户。用户使用他或她拥有的PC(个人计算机，personalcomputer)或盘播放器等再现设备来再现内容，从而使用该内容。

[0005] 通常，内容的创作者或者发行人拥有包括音乐数据和图像数据的很多内容的发行权。因此，当发行这些内容时，一般应用具有预定限制的配置，即，仅允许正规的用户使用该内容，因此未经允许不能进行复制的配置。

[0006] 通过使用数字记录设备和记录介质，可以重复地记录或者再现例如图像或声音，而不使图像或声音劣化。其结果是，通过因特网分发非法复制的内容、分发通过在例如CD-R上复制内容而获得的所谓的盗版盘以及使用存储在PC的硬盘等中的复制内容泛滥。

[0007] 例如，可以将对应于一个或几个电影的大量数据作为数字信息记录在DVD或近年来正在发展的使用蓝色激光的记录介质等大容量记录介质中。因此，由于可以作为数字信息记录视频信息等，因此防止非法复制以保护版权所有者的权利逐渐成为了重要的问题。目前，为了防止数字数据的非法复制，防止使用数字记录设备和记录介质进行非法复制的各种技术已投入实际使用。

[0008] 通过防止非法复制内容来保护版权所有者的权利的技术包括内容加密方法。然而，即使内容被加密，也会出现如果加密密钥泄漏则非法解密内容被散布的问题。

[0009] 此外，作为防止非法使用内容的配置，例如，对希望进行再现的应用程序授予标识符(ID)，从而内容仅能由采用具有特定ID的应用程序的处理来使用。例如，在JP-A-2005-354121中公开了这种配置。此外，作为检查非法产生的内容的产生源的技术，已经提出了一种当再现内容时嵌入进行再现处理的设备的ID的配置。例如，在JP-A-2004-260533中公开了这种配置。

[0010] 在再现内容时进行ID嵌入或内容解密处理等数据转换处理的配置的情况下，可以进行用于检查将要使用内容的信息处理设备或再现（播放）程序是否是有效许可设备或

程序的安全检查或有效性检查。通过执行例如用作内容使用控制程序并与内容一起记录在信息记录介质中的内容代码来进行这些处理。

[0011] 通常，将内容代码设置为与内容独立的文件，然后将内容代码记录在信息记录介质中。因此，可以仅将内容代码移动或复制 到另一个信息记录介质中。如果发生了内容代码泄漏，则具有授权内容使用权的设备之外的未经授权的设备可以通过执行泄漏的内容代码非法地再现内容。

[0012] 将制造商不同的其它设备或应用程序应用于执行内容再现的设备或应用程序。在使用内容代码执行数据转换处理或安全检查的情况下，设置为适当地选择与制造商不同的其它设备或应用程序相对应的内容代码以根据每一个序列执行安全检查并执行适当的数据转换处理是理想的。尤其是，在进行在用不同的数据替换一部分内容数据的数据转换处理期间将执行内容再现的设备或应用程序的识别信息嵌入内容的处理的情况下，如果没有选择正确的内容代码，则不执行正确识别信息的嵌入。其结果是，难以指出执行非法处理的设备。

发明内容

[0013] 因此，针对上述情况，希望实现限制用作内容使用控制程序并与内容一起记录在信息记录介质中的内容代码的使用的配置。具体地，希望提供一种信息处理设备、信息记录介质制造设备、信息记录介质、信息处理方法、信息记录介质制造方法及计算机程序，其用于基于指定用作内容使用设备的信息处理设备的装置、型号或版本等识别信息进行设备检查处理，然后在使用内容代码进行处理时根据设备检查信息准确地选择并执行对应于该信息处理设备的内容代码。

[0014] 根据本发明的第一实施例，提供一种信息处理设备，包括：数据处理单元，其获取包含记录在信息记录介质中的数据处理程序的内容代码，根据该内容代码执行数据处理；以及存储器，其存储包含信息处理设备的设备标识符的设备证书。数据处理单元被配置为根据包含在内容代码中的用于设备检查处理的代码应用存储在存储器中的设备证书执行设备检查处理，在设备检查处理之后获取记录在设备证书中的设备标识符，应用对应于所获得的设备标识符的内容代码执行数据处理。

[0015] 在根据本发明第一实施例的信息处理设备中，优选地，设备证书是存储有信息处理设备特有的装置标识符和装置专用密钥的装置证书，或者是存储有对应于信息处理设备的型号或版本的型号标识符或版本标识符和型号/版本公共密钥的型号/版本证书。此外，优选地，数据处理单元被配置为应用装置证书和型号/版本证书中的至少一个来执行设备检查处理，获取记录在装置证书中的装置标识符与记录在型号/版本证书中的型号标识符/版本标识符中的任意一个，应用对应于所获得的标识符的内容代码执行数据处理。

[0016] 此外，在根据本发明第一实施例的信息处理设备中，优选地，数据处理单元被配置为通过验证在设备证书中设置的签名的处理来检查设备证书的有效性，通过使用存储在信息处理设备的存储器中的专用密钥来产生新的签名数据，通过使用存储在设备证书中的公共密钥来验证所产生的签名数据，执行将签名验证成功判断为设备检查成功的设备检查处理。

[0017] 此外，在根据本发明第一实施例的信息处理设备中，优选还包括：存储器，其存储

在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的节点相对应地设置的组密钥、以及与顶层节点相对应地设置的装置制造实体密钥作为对应于装置和组的数据，存储与信息处理设备的型号／版本相对应的型号密钥／版本密钥作为型号／版本包，并存储密钥管理中心公共密钥，此外，优选地，数据处理单元被配置为应用密钥管理中心公共密钥执行验证内容代码的签名的处理，在应用内容代码的数据处理中 应用装置特有密钥、组密钥、装置制造实体密钥、型号密钥和版本密钥中的任意一个执行解密包含在内容代码中的数据的处理。

[0018] 此外，在根据本发明第一实施例的信息处理设备中，优选地，数据处理单元被配置为从存储在信息记录介质中的数据中获取在内容代码的解密中应用的密钥指定信息和表示在内容代码中设置的加密数据的位置的加密数据位置指定信息，根据获得的信息选择要应用的密钥，根据加密数据位置指定信息指定要解密的数据，应用所选择的密钥执行解密处理。

[0019] 此外，在根据本发明第一实施例的信息处理设备中，优选地，内容代码具有以作为包含在内容代码中的数据的大小为 2MB 的块为单位设置签名的数据结构，数据处理单元被配置为以大小为 2MB 的块为单位执行验证内容代码的签名的处理。

[0020] 此外，在根据本发明第一实施例的信息处理设备中，优选地，在存储器中存储与对应于信息处理设备的制造商、组件的制造商或组装者的多个不同的装置制造实体相对应的独立密钥集，数据处理单元被配置为在进行解密内容代码的处理时，从对应于与要执行的内容代码相对应地选择的装置制造实体的密钥集中选择密钥，从而执行应用所选择的密钥解密包含在内容代码中的数据的处理。

[0021] 此外，在根据本发明第一实施例的信息处理设备中，优选地，数据处理单元被配置为至少执行应用包含在内容代码中的安全检查代码的安全检查处理和应用包含在内容代码中的数据转换表的内容形成数据的数据转换处理中的一个，作为在设备检查处理之后执行的应用内容代码的数据处理。

[0022] 此外，在根据本发明第一实施例的信息处理设备中，优选地，信息处理设备被配置为将存储有与信息处理设备的型号／版本相对应的型号／版本公共密钥的型号／版本证书存储在存储器中，数据处 理单元被配置为通过检查记录在型号／版本证书中的证书更新信息来确定内容代码的应用状态。

[0023] 此外，根据本发明的第二实施例，提供一种信息记录介质制造设备，包括：内容文件产生装置，用于产生存储记录在信息记录介质中的内容数据的内容文件；内容代码文件产生装置，用于产生存储包含当使用内容时所执行的数据处理程序的内容代码的内容代码文件；以及记录装置，用于在信息记录介质中记录内容文件产生装置产生的内容文件和内容代码文件产生装置产生的内容代码文件。内容代码文件产生装置被配置为产生存储有使得执行应用存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的用于设备检查处理的代码的内容代码文件，和产生存储有根据设备检查处理检查后的设备标识符选择并执行的安全检查代码的内容代码文件。

[0024] 在根据本发明第二实施例的信息记录介质制造设备中，优选地，内容代码文件产生装置被配置为产生存储有在根据设备检查处理检查后的设备标识符选择并执行的内容的数据转换处理中所应用的数据转换表的内容代码文件。

[0025] 此外，在根据本发明第二实施例的信息记录介质制造设备中，优选地，内容代码文件产生装置被配置为产生存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件。

[0026] 此外，在根据本发明第二实施例的信息记录介质制造设备中，优选地，加密密钥对应于在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应的型号密钥和与信息处理设备的版本相对 应的版本密钥中的任意一个。

[0027] 此外，在根据本发明第二实施例的信息记录介质制造设备中，优选地，内容代码文件产生装置被配置为执行如下处理：产生作为要在信息记录介质中记录的信息的加密数据部分和包含密钥指定信息的内容代码加密信息，作为与存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件相对应的信息。

[0028] 此外，根据本发明的第三实施例，提供一种信息记录介质，包括：存储有内容数据的内容文件；以及存储有包含当使用内容时所执行的数据处理程序的内容代码的内容代码文件。内容代码文件被配置为包含存储有使得执行应用存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的用于设备检查处理的代码的内容代码文件，和存储有根据设备检查处理检查后的设备标识符选择并执行的安全检查代码的内容代码文件。

[0029] 在根据本发明第三实施例的信息记录介质中，优选地，内容代码文件被配置为包含在根据设备检查处理检查后的设备标识符选择并执行的内容的数据转换处理中所应用的数据转换表。

[0030] 此外，在根据本发明第三实施例的信息记录介质中，优选地，内容代码文件是存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥来进行解密的加密数据的内容代码的内容代码文件。

[0031] 此外，在根据本发明第三实施例的信息记录介质中，优选地，加密密钥对应于在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应的型号密钥和与信息处理设备的版本相对应的版本 密钥中的任意一个。

[0032] 此外，在根据本发明第三实施例的信息记录介质中，优选地，作为与存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥来解密的加密数据的内容代码的内容代码文件相对应的信息，包含加密数据部分和包含密钥指定信息的内容代码加密信息作为记录信息。

[0033] 此外，根据本发明的第四实施例，一种应用信息处理设备中的信息记录介质的记录数据执行数据处理的信息处理方法包括如下步骤：在数据处理单元中获取包含记录在信息记录介质中的数据处理程序的内容代码；在数据处理单元中根据包含在内容代码中的用于设备检查处理的代码应用存储在存储器中的设备证书执行设备检查处理；以及在数据处理单元中执行内容代码处理，在内容代码处理中，获取记录在设备证书中的设备标识符，选择对应于获得的设备标识符的内容代码，应用所选择的内容代码执行数据处理。

[0034] 在根据本发明第四实施例的信息处理方法中，优选地，设备证书是存储有信息处理设备特有的装置标识符和装置专用密钥的装置证书，或者是存储有对应于信息处理设备的型号或版本的型号标识符或版本标识符和型号／版本公共密钥的型号／版本证书。此外，优选地，在执行设备检查处理中，执行应用装置证书和型号／版本证书中的至少一个的设备检查处理，获取记录在装置证书中的装置标识符与记录在型号／版本证书中的型号标识符／版本标识符中的任意一个。此外，在执行内容代码处理中，执行应用对应于所获得的标识符的内容代码的数据处理。

[0035] 此外，在根据本发明第四实施例的信息处理方法中，优选地，在执行设备检查处理中，通过验证在设备证书中设置的签名的处理来检查设备证书的有效性，使用存储在信息处理设备的存储器 中的专用密钥来产生新的签名数据，使用存储在设备证书中的公共密钥来验证产生的签名数据，执行将签名验证成功判断为设备检查成功的设备检查处理。

[0036] 此外，在根据本发明第四实施例的信息处理方法中，优选地，信息处理设备包括：存储器，其存储在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥作为对应于装置和组的数据，存储与信息处理设备的型号／版本相对应的型号密钥／版本密钥作为型号／版本包，并存储密钥管理中心公共密钥。此外，优选地，数据处理单元应用密钥管理中心公共密钥执行验证内容代码的签名的处理，在执行内容代码处理中应用装置特有密钥、组密钥、装置制造实体密钥、型号密钥和版本密钥中的任意一个执行解密包含在内容代码中的数据的处理。

[0037] 此外，在根据本发明第四实施例的信息处理方法中，优选地，在执行内容代码处理中，从存储在信息记录介质中的数据中获取在内容代码的解密中应用的密钥指定信息和表示在内容代码中设置的加密数据的位置的加密数据位置指定信息，根据获得的信息选择要应用的密钥，根据加密数据位置指定信息指定要解密的数据，应用所选择的密钥执行解密处理。

[0038] 此外，在根据本发明第四实施例的信息处理方法中，优选地，内容代码具有以作为包含在内容代码中的数据的大小为 2MB 的块为单位设置签名的数据结构，在数据处理单元中以大小为 2MB 的块为单位执行验证内容代码的签名的处理。

[0039] 此外，在根据本发明第四实施例的信息处理方法中，优选地，在执行内容代码处理中，在进行解密内容代码的处理时，从对应于与要执行的内容代码相对应地选择的装置制造实体的密钥集中 选择密钥，从而执行应用所选择的密钥解密包含在内容代码中的数据的处理。

[0040] 此外，在根据本发明第四实施例的信息处理方法中，优选地，在执行内容代码处理中，数据处理单元执行应用包含在内容代码中的安全检查代码的安全检查处理和应用包含在内容代码中的数据转换表的内容形成数据的数据转换处理中的至少一个，作为在设备检查处理之后执行的应用内容代码的数据处理。

[0041] 此外，在根据本发明第四实施例的信息处理方法中，优选地，在数据处理单元中执行通过检查记录在型号／版本证书中的证书更新信息来确定内容代码的应用状态的处理。此外，优选地，信息处理设备被配置为将存储有对应于信息处理设备的型号／版本的型号／版本公共密钥的型号／版本证书存储在存储器中。

[0042] 此外，根据本发明的第五实施例，一种信息记录介质制造设备的信息记录介质制造方法，包括如下步骤：产生存储记录在信息记录介质中的内容数据的内容文件；产生存储包含当使用内容时所执行的数据处理程序的内容代码的内容代码文件；以及在信息记录介质中记录在产生内容文件中产生的内容文件和在产生内容代码文件中产生的内容代码文件。在产生内容代码文件中，产生存储有使得执行应用存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的用于设备检查处理后的代码的内容代码文件，和存储有根据设备检查处理检查后的设备标识符选择并执行的安全检查代码的内容代码文件。

[0043] 在根据本发明第五实施例的信息记录介质制造方法中，优选地，在产生内容代码文件中，产生存储有在根据设备检查处理检查后的设备标识符选择并执行的内容的数据转换处理中应用的数据转换表的内容代码文件。

[0044] 此外，在根据本发明第五实施例的信息记录介质制造方法中，优选地，在产生内容代码文件中，产生存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件。

[0045] 此外，在根据本发明第五实施例的信息记录介质制造方法中，优选地，加密密钥对应于在具有分层结构的密钥树中与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应的型号密钥和与信息处理设备的版本相对应的版本密钥中的任意一个。

[0046] 此外，在根据本发明第五实施例的信息记录介质制造方法中，优选地，在产生内容代码文件中，执行如下处理：产生作为要在信息记录介质中记录的信息的加密数据部分和包含密钥指定信息的内容代码加密信息，作为与存储有包含仅由分配到使用内容的特定信息处理设备的组的加密密钥进行解密的加密数据的内容代码的内容代码文件相对应的信息。

[0047] 此外，根据本发明的第六实施例，一种使信息处理设备执行应用信息记录介质的记录数据的数据处理的计算机程序使信息处理设备执行：通过数据处理单元获取包含记录在信息记录介质中的数据处理程序的内容代码；通过数据处理单元根据包含在内容代码中的用于设备检查处理的代码应用存储在存储器中的设备证书执行设备检查处理；以及通过数据处理单元执行内容代码处理，在内容代码处理中，获取记录在设备证书中的设备标识符，选择对应于获得的设备标识符的内容代码，执行应用所选择的内容代码的数据处理。

[0048] 此外，根据本发明的第七实施例，提供一种信息处理设备，包括：第一存储器，其存储包含每一个信息处理设备特有的数据的数据；以及第二存储器，其存储与信息处理设备的共有型号和版本相对应的共有数据。包含每一个信息处理设备特有的数据的数据包括包含设备标识符的设备证书、对应于装置制造实体的密钥、将设备划分为组时所设定的预定组共有的组密钥以及每一个设备特有的密钥。与共有型号和版本相对应的共有数据包括型号特有的密钥、版本特有的密钥和包含型号和版本的标识符的设备证书。

[0049] 在根据本发明第七实施例的信息处理设备中，优选地，根据获得的程序，执行基于设备证书的第一签名验证，然后对应于第一签名验证的结果进一步执行使用设备特有的密钥的签名验证，执行基于包含型号和版本标识符的设备证书的第二签名验证，然后对应于第二签名验证的结果进一步执行使用型号特有的密钥或版本特有的密钥的签名验证。

[0050] 此外，根据本发明第六实施例的计算机程序是可以通过使用存储介质或通信介质供给能够执行多种程序 / 代码的计算机 / 系统的计算机可读格式的计算机程序。例如，通过使用 CD、FD 或 MO 等记录介质或者网络等通信介质来提供计算机程序。通过提供计算机可读格式的程序，在计算机 / 系统中实现对应于该程序的处理。

[0051] 通过以下在本发明的实施例中参考附图进行的详细说明，本发明的其它用途、特征和优点将变得明显。此外，说明书中的系统是多个装置的逻辑组。即，不限于在同一机壳中已有的装置。

[0052] 根据根据本发明实施例的配置，在获取包含记录在信息记录介质中的数据处理程序的内容代码、然后根据相应内容代码执行安全检查处理、对包含在内容中的数据的转换处理或将设备信息嵌入内容的处理等数据处理的配置中，执行应用存储在信息处理 设备中的装置证书或型号 / 版本证书的设备检查处理作为检查信息处理设备的处理，在设备检查处理之后获取存储在装置证书或型号 / 版本证书中的用作设备标识符的装置 ID、型号 ID 或版本 ID，在进行应用内容代码的处理时执行应用对应于获得的设备标识符的内容代码的数据处理。

[0053] 此外，根据本发明另一个实施例的配置，将内容代码的至少一部分设置为加密数据，在具有分层结构的密钥树中，作为加密密钥应用包含与作为信息处理设备所对应的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的每一个节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号和版本相对应地设置的型号和版本密钥的加密密钥中的一个。因此，可以仅允许特定信息处理设备的组对内容代码执行处理。其结果是，可以实现能够防止应用非法内容代码的处理的配置。

附图说明

[0054] 图 1 是说明信息记录介质的存储数据、驱动设备和信息处理设备的配置和处理的视图；

[0055] 图 2 是说明对信息记录介质的存储内容设置的内容管理单元的设置例子的视图；

[0056] 图 3 是说明对信息记录介质的存储内容设置的单元密钥和内容管理单元之间的对应关系的视图；

[0057] 图 4 是说明记录在信息记录介质中的内容和在再现内容时所需的数据转换处理的视图；

[0058] 图 5 是说明内容再现处理的例子的视图；

[0059] 图 6 是说明在再现内容时所执行的数据转换处理的视图；

[0060] 图 7 是示出记录在信息记录介质中的数据的目录配置的视图；

[0061] 图 8 是示出记录在信息记录介质中的内容、管理数据等的目录配置的视图；

[0062] 图 9 是示出记录在信息记录介质中的内容代码的目录配置的视图；

[0063] 图 10A 是说明装置证书的数据结构的例子的视图；

[0064] 图 10B 是说明型号 / 版本证书的数据结构的例子的视图；

[0065] 图 11 是说明证书信息和分配到信息处理设备的密钥的视图；

[0066] 图 12 是说明存储在信息处理设备中的证书信息和密钥的视图；

[0067] 图 13 是说明证书信息和分配到信息处理设备的密钥的视图；

[0068] 图 14 是说明更新型号 / 版本证书的处理的视图；

[0069] 图 15 是说明每一个装置制造实体的密钥和证书设置的配置的视图；

[0070] 图 16 是说明每一个装置制造实体的密钥和证书设置的配置的视图；

[0071] 图 17 是说明在密钥管理中心产生密钥和证书的处理的视图；

[0072] 图 18 是说明在密钥管理中心设置对应于内容代码的签名的处理的视图；

[0073] 图 19 是说明在密钥管理中心设置对应于内容代码的签名的处理的视图；

[0074] 图 20 是说明在信息处理设备中内容代码的使用的视图；

[0075] 图 21 是说明产生并加密存储在信息记录介质中的内容代码的处理的视图；

[0076] 图 22 是说明在信息处理设备中使用内容代码的处理序列的视图；

[0077] 图 23 是说明在信息处理设备中使用内容代码的处理序列的视图；

[0078] 图 24 是示出说明在信息处理设备中应用内容代码的处理序列的流程图的视图；

[0079] 图 25 是示出说明在信息处理设备中应用内容代码的处理序列的流程图的视图；

[0080] 图 26 是示出信息处理设备的硬件配置的例子的视图；以及

[0081] 图 27 是说明信息记录介质制造设备的配置的框图。

具体实施方式

[0082] 下文中，参考附图详细说明根据本发明实施例的信息处理设备、信息记录介质制造设备、信息记录介质、信息处理方法、信息记录介质制造方法及计算机程序。此外，将按照如下项目的顺序进行说明。

[0083] 1. 信息记录介质的存储数据及驱动 (drive) 和主机 (host) 中的处理的概要

[0084] 2. 内容管理单元 (CPS 单元)

[0085] 3. 包含变形数据的内容的数据结构和数据转换处理的概要

[0086] 4. 内容再现处理

[0087] 5. 应用安全检查代码的处理

[0088] 6. 对信息处理设备分配加密密钥的配置及内容代码的加密和使用

[0089] 7. 信息处理设备的配置

[0090] 8. 信息记录介质制造设备和信息记录介质

[0091] 1. 信息记录介质的存储数据及驱动和主机中的处理的概要

[0092] 首先，说明信息记录介质的存储数据及驱动和主机中的处理的概要。图 1 示出存储有内容的信息记录介质 100、驱动 (drive)120 和主机 (host)140 的配置。主机 140 是在 PC 等信息处理设备中执行的数据再现 (或记录) 应用程序。主机 140 根据预定数据处理序列使 用 PC 等信息处理设备的硬件进行处理。

[0093] 信息记录介质 100 是蓝光盘 (注册商标) 或 DVD 等信息记录介质，包括在被授予内容版权或发行权的所谓的内容权利持有者的许可下在盘制造厂中制造的数据可记录信息记录介质 (例如，RE 盘) 或者存储有授权内容的信息记录介质 (例如，ROM 盘)。此外，在以下实施例中，作为信息记录介质的例子来说明盘型介质；然而，可以在使用各种信息记录介质的配置中应用本发明。

[0094] 如图 1 所示，信息记录介质 100 存储对部分数据进行了加密处理和替换处理的加

密内容 101、用作加密密钥块并根据已知的作为广播加密方法的树结构密钥分配方法产生的MKB(媒体密钥块,media key block)102、包含通过对应用于内容加密处理的标题密钥进行加密而获得的加密 CPS 单元密钥的标题密钥文件 103、包含作为复制和再现内容的控制信息的 CCI(复制控制信息,copycontrol information)的使用许可信息 104 以及包含使用加密内容 101 时所执行的数据处理程序的内容代码 105。

[0095] 内容代码 105 包括注册有与内容的预定区域中的替换数据相对应的转换数据的转换表(修正(Fix-Up)表)106 以及具有用于验证进行内容再现的播放器(再现设备)的有效性的程序的安全检查代码 107。此外,内容代码 105 包括用于信息处理设备的设备检查的设备检查代码 108,即,根据型号标识符(型号 ID)、版本标识符(版本 ID)或装置标识符(装置 ID)来指定对应于信息处理设备的例如型号、版本或装置的设备检查代码 108。

[0096] 在进行内容再现的信息处理设备中,根据包含在内容代码 105 中的安全检查代码 107 进行验证播放器(再现设备)的有效性的验证处理,在验证处理之后,根据包含在内容代码 105 中的数据转换处理程序提取记录在包含在内容代码 105 中的转换表(Fix-up 表)106 中的转换数据,以对包含在内容中的数据进行替换处理。

[0097] 此外,转换表(Fix-up 表)106 或安全检查代码 107 包括允许根据各种再现设备或再现应用程序的类型进行处理即可以执行安全检查处理或转换处理的各种代码。例如,各种代码包括与在“A”公司中制造的产品的型号 A1、版本 a2 和装置 Aa3 相对应的安全检查代码和转换表以及与在“B”公司中制造的产品的型号 B1、版本 b2 和装置 Bb3 相对应的安全检查代码和转换表。希望使用内容的设备从该安全检查代码或转换表中选择相应的安全检查代码或转换表以进行处理。

[0098] 使用内容的信息处理设备从中选择相应的适当安全检查代码或转换表以进行处理。例如,根据包含对应于信息处理设备的“装置”、定义为多个装置的组的“型号”或型号的下一级概念的“版本”的信息处理设备所属的不同的组,选择适当的安全检查代码或转换表以进行处理。例如,将装置标识符设置为每一个信息处理设备特有的标识符。

[0099] 将型号标识符设置为属于同一型号的多个装置(信息处理设备)共有的。

[0100] 版本标识符是对属于同一型号的不同版本设置的标识符。例如,假设存在型号 A 的版本 1 和型号 A 的版本 2,对应于各版本设置独立的版本标识符。

[0101] 信息处理设备通过应用设备检查代码 108 的处理来检查该信息处理设备所属的信息处理设备的装置、型号、版本等,然后选择适当的转换表或安全检查代码,以进行处理。因此,需要检查相应设备的装置标识符、型号标识符或版本标识符。在设备检查代码 108 中包含用于执行检查处理的设备检查处理程序。

[0102] 希望使用内容的信息处理设备获取存储在信息处理设备的存储器(图 1 所示的存储器 b161)中的装置证书(Device Cert)或型号/版本证书(MV Cert),执行包含在内容代码 105 中的设备检查代码 108,执行检查信息处理设备的装置、型号或版本的处理。在设备检查处理之后,信息处理设备选择对应于确认的装置、型号或版本的适当的安全检查代码或转换表以进行处理。装置证书(DeviceCert)或型号/版本证书(MV Cert)是存储有公共密钥的公共密钥证书。稍后说明该处理的具体处理例子。

[0103] 此外,内容代码 105 除了包含应用转换数据的转换处理程序之外,还包含用于执行启动处理和安全检查处理等多种处理的信息或程序。稍后说明内容代码的细节。此外,

图中所示的信息记录介质存储数据是例子，存储数据根据盘等的类型而稍有不同。下文中，说明各种信息的概要。

[0104] (1) 加密内容 101

[0105] 在信息记录介质 100 中存储各种内容。例如，各种内容包括作为高清晰度运动图片数据的 HD（高清晰度，high definition）电影内容等运动图片内容的 AV（视听，audio visual）流、或者包含以特定标准指定的游戏程序、图像文件、声音数据或文本数据的内容。这些内容是特定 AV 格式标准数据，根据特定 AV 数据格式对其进行存储。具体地，例如，根据蓝光盘（注册商标）ROM 标准格式将内容存储为蓝光盘（注册商标）ROM 标准数据。

[0106] 此外，例如，可以在信息记录介质 100 中存储用作服务数据的游戏程序、图像文件、声音数据或文本数据。可以将这些内容存储为具有不遵循特定 AV 数据格式的数据格式的数据。

[0107] 存在包括音乐数据、运动图片和静止图像等图像数据、游戏程序和 WEB 内容的各种内容。内容包括仅可以由来自信息记录介质 100 的数据使用的各种内容信息以及可以由来自信息记录介质 100 的数据和从连接到网络的服务器供给的数据使用的内容信息。对于存储在信息记录介质中的内容，在对独立内容分配不同的密钥 (CPS 单元密钥或单元密钥（或者通常称为标题密钥）) 的状况下 加密内容，然后存储该内容，以实现对独立内容的不同使用控制。将分配了一个单元密钥的单元称为内容管理单元 (CPS 单元）。此外，将包含在内容中的一部分数据设置为使用与正确的内容数据不同的数据替换的数据片断。因此，由于仅用解密处理不能再现正确的内容，因此需要用在转换表中注册的数据来替换数据片断的处理以执行再现。稍后详细说明该处理。

[0108] (2)MKB

[0109] MKB（媒体密钥块）102 是根据已知的作为广播加密方法的树结构密钥分配方法产生的加密密钥块。MKB102 是仅允许通过基于存储在具有有效许可的用户的信息处理设备中的装置密钥 [Kd] 的处理（解密）来获得的作为解密内容所需的密钥的媒体密钥 [Km] 的密钥信息块。对其应用根据所谓的分层树结构的信息分配方法。即，仅当用户装置（信息处理设备）具有有效许可时，可以获得媒体密钥 [Km]，但是在用户装置无效（废止）的情况下，不能获得媒体密钥 [Km]。

[0110] 作为许可实体的管理中心可以通过改变用于加密存储在 MKB 中的密钥信息的装置密钥来产生具有不能使用存储在特定用户装置中的装置密钥解密、即不能获取解密内容所需的媒体密钥的配置的 MKB。因此，可以仅向具有有效许可的装置提供可以解密的加密内容，同时在预定定时废止未经授权的装置。稍后说明内容的解密处理。

[0111] (3) 标题密钥文件

[0112] 如上所述，通过在使用内容时应用用于管理的独立加密密钥（标题密钥 (CPS 单元密钥)）来加密内容中的每一个或者多个内容的一组，然后，将其存储在信息记录介质 100 中。即，可以将包含在内容中的 AV（视听）流、音乐数据、运动图片和静止图像等图像数据、游戏程序、WEB 内容等划分为作为使用内容的管理单位的 单元。此外，需要针对各划分后的单元产生不同的标题密钥并进行解密处理。用于产生标题密钥的信息是标题密钥数据。例如，通过使用由媒体密钥等产生的密钥对加密标题密钥进行解密来获得标题密钥。根据应用了标题密钥数据的预定加密密钥产生序列来产生对应于每一个单元的标题密钥，从而

进行内容的解密。

[0113] (4) 使用许可信息

[0114] 用户许可信息例如包括复制和再现控制信息 (CCI)。即，复制和再现控制信息 (CCI) 是用于与存储在信息记录介质 100 中的加密内容 101 相对应的使用控制的复制限制信息或再现限制信息。例如，可以将复制和再现控制信息 (CCI) 设置为作为内容管理单元而设置的独立 CPS 单元的信息，或者可以与多个 CPS 单元相对应地设置复制和再现控制信息 (CCI)。即，可以以各种方式设置复制和再现控制信息 (CCI)。

[0115] (5) 内容代码

[0116] 内容代码 105 包括注册有与内容的预定区域中的替换数据相对应的转换数据的转换表 (Fix-up 表)106 以及具有用于验证进行内容再现的信息处理设备的有效性的程序的安全检查代码 107。此外，如上所述，内容代码 105 包括用于检查与信息处理设备相对应的装置、型号和版本中的至少一个的识别信息的设备检查代码 108。

[0117] 如上所述，转换表或安全检查代码包括各种代码以可以进行对应于用作各种再现设备的信息处理设备 (例如，装置、型号或版本) 的类型的处理。希望使用内容的信息处理设备根据设备检查代码 108 检查信息处理设备的装置、型号、版本等，然后选择对应于信息处理设备的安全检查代码或转换表以进行安全检查处理和数据转换处理。

[0118] 执行内容再现的作为再现设备的再现应用程序的主机设置执 行数据转换处理的虚拟机 (VM，virtual machine)，在虚拟机 (VM) 中根据从信息记录介质 100 中读出的内容代码执行设备检查处理、安全检查处理和数据转换处理，通过应用转换表 (Fix-up 表)106 的注册项对包含在内容中的一部分数据执行数据转换处理。

[0119] 以预定方式加密存储在信息记录介质 100 中的加密内容 101，包含在加密内容 101 中的部分数据包含与正确的数据不同的数据片断。当再现内容时，需要用作为正确内容数据的转换数据来替换该数据片断的数据重写处理。注册有转换数据的表是转换表 (Fix-up 表)106。数据片断的数量设置为根据内容而分散，当再现数据时，需要使用在转换表中注册的转换数据来替换 (重写) 多个数据片断的处理。例如，通过应用转换数据，即使当加密密钥泄漏因而非法执行内容的解密时，由于替换数据也难以仅通过解密内容来再现正确的内容。其结果是，可以防止非法使用内容。

[0120] 此外，转换表 106 除了包括正常的转换数据之外，还包括具有可以分析能够用来识别内容再现设备或内容再现应用程序的识别信息位的数据的转换数据 (司法标记 (forensic mark))。具体地，转换表 106 例如包含 :用作对应于信息处理设备的识别数据的装置 ID(装置标识符)、型号 ID(型号标识符) 或版本 ID(版本标识符) 等标识符，或者记录有根据标识符信息而产生的识别信息的“包含识别标记的转换数据 (司法标记)”。包含识别标记的转换数据是通过以不影响内容的再现的水平稍微改变正确的内容数据的位值而获得的数据。

[0121] 此外，内容代码 105 除了包含应用上述转换表 106 的数据转换处理程序之外，还包含用于执行启动处理和安全检查处理等多种处理的信息或程序。稍后说明内容代码的细节。

[0122] 接下来，参考图 1 说明主机 140 和驱动 120 的配置和其处理的概要。当将数据通过驱动 120 发送到主机 140 时，执行对存储在信 息记录介质 100 中的内容的再现处理。

[0123] 在主机 140 中设置再现（播放器）应用程序 150 和安全 VM160。再现（播放器）应用程序 150 是内容再现处理单元，在内容再现处理、内容解密处理、解码处理等中进行主机 140 和驱动之间的认证处理。

[0124] 安全 VM160 是进行应用内容代码 105 的处理的数据处理单元。内容代码 105 包含转换表 106、安全检查代码 107 和设备检查代码 108。安全 VM160 根据设备检查代码 108 进行包含设备的型号、版本和装置的设备检查，选择对应于检查后的设备的安全检查代码 107，然后进行安全检查处理，使用转换表 106 进行内容的一部分数据的替换处理。

[0125] 用作数据处理单元的安全 VM160 根据包含在内容代码中的设备检查代码 108 执行应用存储在存储器中的设备证书（装置证书和型号 / 版本证书）的设备检查处理。在设备检查处理之后，安全 VM160 获取记录在设备证书中的设备标识符（型号 ID、版本 ID 和装置 ID），进行应用对应于所获得的设备标识符的内容代码的数据处理。

[0126] 此外，将安全 VM160 设置为主机 140 内的虚拟机。虚拟机 (VM) 是直接分析并执行中间语言的虚拟计算机。虚拟机 (VM) 从信息记录介质 100 中读出不取决于平台的中间语言的命令代码信息，然后分析并执行该信息。

[0127] 安全 VM160 用作获取记录在信息记录介质 100 中的包含所应用的信息或在使用加密内容 101 时所应用的程序的内容代码 105 的数据处理单元，根据获得的内容代码 105 执行数据处理。

[0128] 安全 VM160 从作为安全 VM 可访问的存储器的存储器 b161 中获取装置证书 (Device Cert) 或型号 / 版本证书 (MV Cert) 等设备信息，通过应用该证书来进行设备检查处理，即进行根据装置、型号或版本等标识符来检查设备的处理，根据所检查的设备识别信息从信息记录介质中选择对应于该设备的适当的内容代码，然后执行所选择的内容代码。

[0129] 此外，将一部分内容代码设置为加密数据，将解密加密数据的加密密钥存储在存储器 b161 中。安全 VM160 应用从存储器 b161 中选择的密钥对内容代码执行解密处理。

[0130] 例如，将用作装置特有的密钥的装置特有密钥、多个装置的组共有的组密钥、对应于特定设备型号的型号密钥或对应于特定型号的特定版本的版本密钥存储在存储器 b161 中。

[0131] 此外，装置特有密钥和组密钥包括在具有分层结构的密钥树中与从用作信息处理设备所对应的最底层节点的叶片 (leaf) 到顶层节点的路径上的每一个节点相对应地设置的节点密钥。每一个信息处理设备存储节点密钥作为装置特有密钥和组密钥。稍后说明密钥的配置的细节。

[0132] 在解密包含在内容代码中的加密代码的情况下，安全 VM160 从存储器 b161 中选择装置特有密钥、多个装置的组共有的组密钥、型号密钥或版本密钥作为节点密钥，然后应用所选择的密钥对内容代码进行解密处理。此外，稍后说明存储在存储器 b161 中的加密密钥的细节和安全 VM160 的执行的细节。

[0133] 通过再现（播放器）应用程序 150 对安全 VM160 的中断 (INTRP) 序列以及安全 VM160 对再现（播放器）应用程序 150 的应答（呼叫）处理来进行再现（播放器）应用程序 150 和安全 VM160 之间的信息发送或处理请求。通过应用程序 150 对安全 VM160 的中断 (INTRP) 序列以及安全 VM160 对再现（播放器）应用程序 150 的应答（呼叫）处理来进行

信息发送或处理请求。

[0134] 接下来，说明主机 140 执行的主处理。在使用内容之前，执行驱动 120 和主机 140 之间的相互认证。如果通过相互认证确认驱动 120 和主机 140 是有效的，则将加密内容从驱动发送到主机。然后，在主机中，对内容执行解密处理，使用上述转换表执行数据转换处理，从而进行内容再现。

[0135] 驱动 120 的数据处理单元 121 执行当使用内容、从信息记录介质中读取数据、将数据发送到主机的处理等时所执行的驱动 120 和主机之间的认证处理。

[0136] 主机 140 的再现（播放器）应用程序 150 是在 PC 等信息处理设备中执行的数据再现（或记录）应用程序，根据预定数据处理序列使用 PC 等信息处理设备的硬件执行处理。

[0137] 主机 140 包括在主机 140 和驱动 120 之间进行数据发送控制或相互认证处理的数据处理单元 151、对加密内容进行解密处理的解密处理单元 153、基于在转换表 106 中注册的数据进行数据转换处理的数据转换处理单元 154 和进行解码（例如，MPEG 解码）处理的解码处理单元 155。

[0138] 在解密处理单元 153 中，应用存储在存储器 156 中的多种信息和从信息记录介质 100 中读取的数据，产生解密内容要应用的密钥，对加密内容 101 执行解密处理。数据转换处理单元 154 根据从信息记录介质 100 中获得的数据转换处理程序，应用在从信息记录介质 100 中获得的转换表中注册的转换数据对内容的数据的进行替换处理（重写）。解码处理单元 155 进行解码（例如，MPEG 解码）处理。

[0139] 将装置密钥 (Kd)、相互认证处理所应用的密钥信息或解密所应用的密钥信息存储在信息处理设备 150 的存储器 156 中。此外，稍后说明内容的解密处理的细节。装置密钥 (Kd) 是在上述 MKB 的处理中应用的密钥。MKB 是仅允许通过基于存储在具有有效许可的用户的信息处理设备中的装置密钥 [Kd] 的处理（解密）来获得作为解密内容所需的密钥的媒体密钥 [Km] 的密钥信息块。在对加密 内容进行解密时，信息处理设备 150 应用存储在存储器 156 中的装置密钥 (Kd) 对 MKB 进行处理。此外，稍后说明内容的解密处理的细节。

[0140] 2. 内容管理单元 (CPS 单元)

[0141] 如上所述，对于存储在信息记录介质中的内容，在对各单元分配不同的密钥的状况下加密内容，然后进行存储，以实现对各单元的不同的使用控制。即，将内容划分为内容管理单元 (CPS 单元)，对内容管理单元 (CPS 单元) 中的每一个进行独立的加密处理，从而实现独立的使用管理。

[0142] 为了使用内容，首先，需要获取对每一个单元分配的 CP S 单元密钥（也称为标题密钥）。此外，应用其它必要的密钥和用于产生密钥的信息执行基于预定解密处理序列的数据处理，从而进行再现。下文中，参考图 2 说明内容管理单元 (CPS 单元) 的设置。

[0143] 如图 2 所示，内容具有 (A) 索引 210、(B) 电影对象 220、(C) 播放列表 230 和 (D) 剪辑 240 的分层结构。例如，当指定再现应用程序所访问的标题等索引时，指定与标题相关的再现程序，选择根据所指定的再现程序的程序信息指定例如内容的再现顺序的播放列表。

[0144] 播放列表包括作为要再现的数据信息的播放项目。通过包含在播放列表中的播放项目所指定的再现部分的剪辑信息有选择地读出 AV 流或作为实际内容数据的命令，从而进行 AV 流的再现和命令的执行。此外，存在多个播放列表和多个播放项目，用作识别信息

的播放列表 ID 和播放项目 ID 对应于播放列表中的每一个和播放项目中的每一个。

[0145] 图 2 示出两个 CPS 单元。这些 CPS 单元形成存储在信息记录介质中的一部分内容。第一内容单元 271 和第二内容单元 272 每一个都是设置为包含作为索引的标题、作为再现程序文件的电影对象、播放列表和作为实际内容数据的 AV 流文件的单元的 CPS 单元。

[0146] 第一内容管理单元 (CPS 单元)271 包括第一标题 211 和第二标题 212、再现程序 221 和 222、播放列表 231 和 232 以及剪辑 241 和 242。原则上,作为包含在两个剪辑 241 和 242 中的内容的实际数据的 AV 流数据文件 261 和 262 至少是要加密的数据,将其设置为应用作为对应于第一内容管理单元 (CPS 单元)271 设置的加密密钥的标题密钥 (Kt1 ;也称为 CPS 单元密钥) 而加密的数据。

[0147] 第二内容管理单元 (CPS 单元)272 包括第一应用程序 213、再现程序 224、播放列表 233 和剪辑 243 作为索引。应用作为与第二内容管理单元 (CPS 单元)272 相对应地设置的加密密钥的标题密钥 (Kt2) 来加密作为包含在剪辑 243 中的内容的实际数据的 AV 流数据文件 263。

[0148] 例如,用户为了执行对应于第一内容管理单元 271 的内容再现处理或应用程序文件,需要获取作为与第一内容管理单元 (CPS 单元)271 相对应地设置的加密密钥的标题密钥 Kt1,以执行解密处理。为了执行对应于第二内容管理单元 272 的内容再现处理或应用程序文件,需要获取作为与第二内容管理单元 (CPS 单元)272 相对应地设置的加密密钥的标题密钥 Kt2,以执行解密处理。

[0149] 图 3 示出 CPS 单元的设置配置和标题密钥的对应性例子。图 3 示出用作存储在信息记录介质中的加密内容的使用管理单元的 CPS 单元设置单元和应用于每一个 CPS 单元的标题密钥 (CPS 单元密钥) 之间的对应性。此外,可以设置为预先存储后续数据的 CPS 单元和标题密钥。例如,数据单元 281 是后续数据项。

[0150] 存在包含内容的标题、应用程序和数据组的各种 CPS 单元设置单元。此外,在 CPS 单元管理表中将 CPS 单元 ID 设置为对应于各 CPS 单元的标识符。

[0151] 参考图 3,例如,第一标题是第一 CPS 单元。在解密属于第一 CPS 单元 1 的加密内容时,需要产生标题密钥 Kt1 并执行基于所产生的标题密钥 Kt1 的解密处理。

[0152] 如上所述,在对各单元分配不同的密钥的状况下加密存储在信息记录介质 100 中的内容,然后进行存储,以实现对各单元的不同的使用控制。对于对每一个内容管理单元 (CPS 单元) 的独立使用管理,设置使用许可信息 (UR :使用规则 (use rule))。如上所述,使用许可信息是例如包含内容的复制和再现控制信息 (CCI) 的信息,是包含在每一个内容管理单元 (CPS 单元) 中的加密内容的复制限制信息或再现限制信息。

[0153] 此外,需要应用存储在信息记录介质中的多种信息的数据处理以产生标题密钥。稍后详细说明该处理的具体例子。

[0154] 3. 包含变形数据的内容的数据结构和数据转换处理的概要

[0155] 接下来,说明包含变形数据的内容的数据结构和数据转换处理的概要。如上所述,在包含在信息记录介质 100 中的加密内容 101 中,将包含在加密内容 101 中的一部分数据设置为使用与正确的内容数据不同的数据替换的数据片断。因此,由于仅通过解密处理不能再现正确的内容,因此需要使用在转换表中注册的转换数据来替换数据片断的处理以执行再现。

[0156] 参考图 4，说明存储在信息记录介质中的内容的配置和再现处理的概要。将电影等 AV（视听）内容存储在信息记录介质 100 中。稍后将说明如下特定内容再现处理：加密这些内容，通过应用仅可以在具有预定许可的再现设备中获得的加密密钥的处理来解密内容，从而可以再现内容。加密存储在信息记录介质 100 中的内容，该内容具有用变形数据来替换内容的数据的配置。

[0157] 图 4 示出存储在信息记录介质 100 中的记录内容 291 的配置的例子。记录内容 291 包括未变形的正常内容数据 292 和作为由于变形而断裂的内容的数据片断 293。通过使用数据处理使原始内容断 裂而获得数据片断 293。因此，当应用包含数据片断的内容 291 时，无法执行正常的内容再现。

[0158] 为了执行内容再现，需要通过进行使用正常内容数据替换包含在记录内容 291 中的数据片断 293 的处理来产生再现内容 296。通过从在记录在信息记录介质 100 中的内容代码 105 内的转换表 (FUT(Fix-up 表))106（参考图 1）中注册的转换项 295 中获取转换数据、进行在数据片断区域中替换数据的处理、产生再现内容 296，来再现转换为对应于每一个数据片断区域的正常内容数据的数据（转换数据）。

[0159] 此外，当产生再现内容 296 时，进行使用用作正常内容数据的转换数据 297 替换数据片断 293 的处理，以及使用包含可以分析用来识别内容再现设备或内容再现应用程序的识别信息（例如，装置 ID、型号 ID 或版本 ID）位的数据的标识符设置转换数据 298 来替换记录内容 291 的部分区域的处理。例如，在非法复制内容泄漏的情况下，可以通过分析泄漏内容中的标识符设置转换数据 298 来指定非法内容泄漏的原因。

[0160] 此外，可以在内容的数据之间通过特定的包来分配作为包含在包含转换数据的转换表中的数据的转换项，以重复地进行记录。即，将转换数据存储在图 1 所示的转换表 106 中，还将其记录在加密内容 101 中，以进行分配。因此，重复地记录转换数据。执行内容再现的信息处理设备获取存储在转换表 106 中的转换数据以执行数据替换，或者以分配的方式获取记录在内容中的转换项以执行数据替换。

[0161] 4. 内容再现处理

[0162] 接下来，参考图 5 说明主机执行的内容再现处理。参考图 5，从左侧开始按以下顺序示出存储加密内容的信息记录介质 330、设置有信息记录介质 330 并执行数据读取的驱动 340 以及连接到驱动 以与驱动进行数据通信并通过驱动 340 获取存储在信息记录介质 330 中的内容、然后执行用于执行再现处理的再现应用程序的主机 345。

[0163] 此外，在图 5 所示的主机 345 中，彼此独立地示出再现（播放器）应用程序块 350 和具有安全 VM361 的安全 VM 块 360。在再现（播放器）应用程序块 350 中，执行内容的解密和解码、数据转换处理等。安全 VM361 基于包含在记录在信息记录介质中内容代码中的设备检查处理程序来执行设备检查，即，使用装置标识符、型号标识符或版本标识符来指定设备的处理，执行应用于基于安全检查代码的安全检查处理和基于转换表的转换处理的参数计算处理。

[0164] 信息记录介质 330 包括 MKB（媒体密钥块）331、标题密钥块 332、加密内容 333 和内容代码 334 作为记录数据。首先，如先前参考图 4 所说明的，加密内容 333 是需要用从转换表获得的数据替换其一部分的内容。

[0165] 内容代码 334 包括具有用于验证进行内容再现的播放器（再现设备）的有效性的

程序的安全检查代码 335 以及注册有与内容的预定区域中的替换数据相对应的转换数据的转换表 (Fix-up 表)336。主机 345 保持在 MKB 的处理中应用的装置密钥 351。

[0166] 下文中，说明图 5 所示的主机 345 通过驱动 340 获取存储在信息记录介质 330 中的内容、然后再现获得的内容的处理序列。首先，在读取存储在信息记录介质 330 中的内容之前，在步骤 S101 中，主机 345 和驱动 340 进行相互认证。相互认证是检查主机和驱动是否是有效的设备或应用程序软件的处理。可以应用多种处理作为相互认证处理序列。通过相互认证处理，驱动 340 和主机 345 共享用作共有专用密钥的会话 (session) 密钥 (Ks)。

[0167] 在步骤 S101 中在主机和驱动之间进行相互认证以共享会话密钥 (Ks) 之后，在步骤 S102 中，主机 345 的再现 (播放器) 应用程序块 350 通过驱动获取记录在信息记录介质 330 中的 MKB331，通过应用存储在存储器中的装置密钥 351 对 MKB331 执行处理来从 MKB331 中获取媒体密钥 (Km)。

[0168] 如上所述，MKB(媒体密钥块)331 是根据已知的作为广播加密方法的树结构密钥分配方法而产生的加密密钥块。此外，MKB(媒体密钥块)331 是仅允许通过基于存储在具有有效许可的设备中的装置密钥 (Kd) 进行处理 (解密) 而获得作为解密内容所需的密钥的媒体密钥 (Km) 的密钥信息块。

[0169] 然后，在步骤 S103 中，通过应用在步骤 S102 中的 MKB 处理中获得的媒体密钥 (Km) 并执行对从信息记录介质 330 中读出的标题密钥文件 332 的解密来获得标题密钥 (Kt)。存储在信息记录介质 330 中的标题密钥文件 332 是包含用媒体密钥加密的数据的文件。可以通过应用媒体密钥的处理来获得用于内容解密的标题密钥 (Kt)。此外，在步骤 S103 中的解密处理中，例如，应用 AES 加密算法。

[0170] 然后，主机 345 的再现 (播放器) 应用程序块 350 通过驱动 340 读取存储在信息记录介质 330 中的加密内容 333，并读取轨迹 (trace) 缓冲器 352 以存储内容。然后，在步骤 S104 中，应用标题密钥 (Kt) 对存储在缓冲器 352 中的内容进行解密处理，从而获得解密的内容。

[0171] 将解密的内容存储在明码 (plain sentence)TS 缓冲器 353 中。“明码 TS”意为解密了的明码传输流。在这种情况下，存储在明码 TS 缓冲器 353 中的解密内容是包含上述数据片断的内容。因此，应当进行预定数据转换 (通过重写进行数据替换) 以再现解密的内容。

[0172] 在步骤 S105 中，安全 VM361 进行从内容代码 334 中产生数据转换所需的参数等的处理。之后，在步骤 S106 中，通过实时事件 处理机 356 的控制执行表的恢复和数据转换处理。通过实时事件处理机 356 的控制，再现 (播放器) 应用程序块 350 根据包含在内容中的数据段的切换将参数计算请求输出到安全 VM361 作为中断 (INTRP)，随后接收来自安全 VM361 的参数，通过对转换表块进行解密或运算获取明码语句转换表块，获取包含在获得的转换表块中的转换项。

[0173] 在转换项中记录转换数据，即，(a) 转换数据，(b) 标识符设置转换数据 (司法标记)，以及转换数据在内容中的记录位置指定信息。在步骤 S106 中，再现 (播放器) 应用程序块 350 执行作为与内容再现处理或外部输出处理并行的实时处理的用于将转换数据记录在指定位置的数据转换处理。

[0174] 安全 VM361 根据内容代码产生并输出例如应用于作为包含在内容中的数据的各

段的不同参数。例如，在参数 (SP1，SP2，SP3，...) 是与每一个都是与内容的预定部分数据单元的段相对应的转换项进行了异或 (XOR) 运算的参数的情况下，步骤 S106 中的表恢复处理如下。

[0175] [转换项 1](XOR)[SP1]，

[0176] [转换项 2](XOR)[SP2]，

[0177] [转换项 3](XOR)[SP3]，...

[0178] 通过执行异或运算处理来获得包含在转换表块数据中的转换项。此外，在上述表达式中，假设 [A](XOR)[B] 意为 A 和 B 之间进行异或运算。

[0179] 因此，包含在记录在信息记录介质中的内容 333 中的转换项关于参数 (SP1，SP2，SP3，...) 进行异或运算，然后进行存储。随后，安全 VM361 获得该参数并输出。

[0180] 在步骤 S106 中的表恢复和数据转换处理中，从通过应用参数 (SP1，SP2，SP3，...) 的运算或加密处理而获得的解密转换项中获 得转换数据，使用作为包含在内容中的有效数据的转换数据替换包含在内容中的数据片断，进行使用内容的部分数据替换标识符设置转换数据的数据重写处理，将存储在明码 TS 缓冲器 353 中的数据变为转换后的数据。参考图 6 示意性地说明数据转换处理。

[0181] 首先，将存储在信息记录介质中的加密内容 333 存储在主机的轨迹缓冲器 352 中。(1) 图 6 示出轨迹缓冲器存储数据 401。通过主机侧的解密处理来执行将加密内容解密为轨迹缓冲器存储数据 401，将解密结果数据存储在明码 TS 缓冲器 353 中。(2) 图 6 示出解密结果数据 402。

[0182] 解密结果数据 402 包括作为包含在内容中的非正常数据的数据片断 403。主机的数据转换处理单元执行使用作为包含在内容中的正确数据的转换数据 404 替换数据片断 403 的处理。例如，作为再写（重写）来对已完成在明码 TS 缓冲器 353 的记录的数据中的部分数据进行替换处理。

[0183] 此外，在主机执行的数据转换处理中，如图 6 所示，进行使用作为正常内容数据的转换数据来替换数据片断的处理以及通过标识符设置转换数据 405 替换部分解密结果数据 402 的处理。

[0184] 如上所述，标识符是可以分析用来识别内容再现设备或内容再现应用程序的识别信息位的数据。具体地，标识符例如是根据包含在用作执行主机应用程序的播放器的信息处理设备的识别信息（例如，装置 ID、型号 ID 或版本 ID) 中的数据而产生的标识标记，或者是 ID。如上所述，标识符设置转换数据是通过以不影响再现内容的水平稍微改变正确内容数据的位值而获得的数据。

[0185] 在内容中设置多个标识符设置转换数据 405，例如，通过总体地分析该多个标识符设置转换数据 405 来确定装置 ID。例如，将装置 ID 设置为信息处理设备所特有的标识信息，可以通过总体分析标识符设置转换数据 405 来指定信息处理设备。标识符设置转换数据 405 是通过以可以正常再现内容的水平改变形成正常内容数据的位而获得的数据。此外，标识符设置转换数据 405 是可以通过 MPEG 位流分析来确定位（识别标记形成位）的数据。

[0186] 在存储在信息记录介质中的转换表中，注册有图 6 所示的多个转换数据 404 和多个设置转换数据 405，还注册有其记录位置信息。通过基于存储在转换表中的信息的数据转

换处理，使用图 6 中的 (3) 转换完成数据 406 替换存储在明码 TS 缓冲器 353 中的数据。

[0187] 然后，将转换完成 TS(传输流，transport stream) 通过网络等输出到外部，然后在外部再现设备中进行再现。可选地，在步骤 S107 中，通过使用解复用器的处理进行从传输流 (TS) 到基本流 (ES，elementary stream) 的转换，然后进行解码处理 (步骤 S108) 以通过显示扬声器进行再现。

[0188] 5. 应用安全检查代码的处理

[0189] 在开始上述内容再现处理之前，安全 VM361 获取存储在信息处理设备的存储器 (图 1 所示的存储器 b161) 中的证书，即装置证书 (Device Cert) 或型号 / 版本证书 (MV Cert)，执行包含在内容代码中的设备检查代码，即用于检查装置、型号或版本的程序代码，执行检查相应设备的装置、型号或版本的处理，然后选择适当的转换表或对应于检查后的装置、型号或版本的安全检查代码以进行处理。此外，如果需要，即使正在执行内容再现处理时，安全 VM361 也应用安全检查代码 335 执行安全检查。

[0190] 安全 VM361 在事件处理机 354 的控制下根据包含在内容代码 334 中的安全检查代码 335 执行验证播放器 (再现设备) 的有效性的处理。此外，如上所述，将转换表 (Fix-up 表)336 或安全检查代码 335 设置为包含各种代码从而使得可以根据作为再现设备的播放器的类型执行处理。

[0191] 安全 VM361 根据通过获取存储在再现设备的存储单元中的 用作播放器信息 335 的各种证书即装置证书 (Device Cert) 或型号 / 版本证书 (MV Cert) 而执行的设备检查处理所确认的设备信息，从包含在内容代码 334 中的安全检查代码 335 中选择与安全 VM361 所属的信息处理设备相对应的安全检查代码，然后执行安全检查处理。即，选择对应于识别信息的安全检查代码或对应于信息处理设备的属性信息，然后执行基于所选择的安全检查处理。

[0192] 在安全 VM361 的安全检查中，如果根据设备信息证实设备是允许使用内容的有效设备并且没有向外部非法输出内容，则执行内容的再现。

[0193] 可以根据再现设备的配置和应用程序的类型来请求不同的安全检查。因此，将安全检查代码记录在内容代码中作为对应于各种设备或应用程序的一组代码。

[0194] 接下来，参考附图说明在信息记录介质中记录内容代码的方法。图 7 是示出存储在信息记录介质中的整个数据的目录配置的视图。将存储在信息记录介质中的数据大致划分为两个数据项目。一个是设置有包含内容管理数据、CPS 单元密钥、内容使用控制信息 (CCI) 和内容的内容相关数据的 BDMV 目录，另一个是设置有包含安全检查代码和转换表的内容代码的 BD SVM 目录。

[0195] 参考图 8 和 9 说明目录的详细例子。首先，在将上述参考图 2 所说明的具有分层结构的内容存储在信息记录介质的情况下，根据图 8 所示的目录设置将例如作为独立文件所记录的内容代码等各种数据或程序存储在信息记录介质中。

[0196] (A) 图 2 中的索引 210 是图 8 所示的目录中的 index.bdmv 文件

[0197] (B) 图 2 中的电影对象 220 是图 8 所示的目录中的 MovieObject.bdmv 文件

[0198] (C) 图 2 中的播放列表 230 是图 8 所示的目录中的属于 PLAYLIST 目录的文件

[0199] (D) 图 2 中的剪辑 240 是图 8 所示的目录中的属于 CLIPINF 目录的文件和属于 STREAM 目录的文件，其中，属于 CLIPINF 目录的文件和属于 STREAM 目录的文件具有相同的

文件数量，并成对地彼此对应。

[0200] (E) 其它，例如，将存储声音数据或字体数据的 AUXDATA 文件、存储元数据 (metadata) 的 MATA 文件和存储 BD-J 对象的 BDJO 文件存储在信息记录介质中。

[0201] 如上所述，将包含在存储在信息记录介质中的内容中的部分数据设置为用与正确内容数据不同的数据替换的数据片断。因此，由于仅通过解密处理不再现正确的内容，因此需要用在转换表中注册的数据（转换数据）替换数据片断的处理以执行再现。在替换处理中，应用存储在信息记录介质中的内容代码，执行基于在转换表 (Fix-up 表）中注册的数据的数据转换处理。

[0202] 也将转换表和包含安全检查代码的内容代码作为独立的文件存储在信息记录介质中。图 9 示出设置有内容代码的目录的配置。图 9 示出例如对具有图 8 中的目录配置的 AV 内容产生的内容代码的目录配置。

[0203] 如上所示，内容代码包括安全检查代码、转换表和用于设备检查的代码。如图 9 所示，将存储在信息记录介质中的内容代码存储在设置在 BDSVM 目录中的多个独立文件 [nnnnn.svm] 中。此外，将备份数据作为副本数据设置在 BACKUP 目录中。

[0204] 如图 9 所示，内容代码文件包括以下类型的文件。

[0205] 内容代码文件 [00000.svm] ：应用于装置、型号和版本信息的判断的代码

[0206] 内容代码文件 [00001.svm] 和 [00002.svm] ：根据设备信息选择的代码（例如，00001.svm 是型号 A 的代码，00002.svm 是型号 B 的代码）

[0207] 内容代码文件 [00003.svm] ：不取决于设备信息的处理（例如，对释放内容之后所售出的设备执行在 00003.svm 中公开的默认代码）。

[0208] 例如，将内容代码文件分类为以下种类 (a) ～ (d)。

[0209] (a) 全部内容和全部装置共有的内容代码

[0210] (b) 内容特有的内容代码

[0211] (c) 装置、型号或版本特有的内容代码

[0212] (d) 内容和设备特有的内容代码（例如，装置、型号或版本）

[0213] 将作为应用于根据每一个识别信息检查与希望执行内容再现的信息处理设备相对应的装置、型号和版本的代码的设备检查处理所执行的代码即设备检查代码设置为全部内容和全部装置共有的内容代码。信息处理设备应用该代码执行检查型号、版本或装置的处理。根据作为检查结果所获得的设备信息，信息处理设备基于来自上述 (a) ～ (d) 的每一种代码的对应于信息处理设备的安全检查代码进行安全检查处理，执行包含基于对应于信息处理设备的转换表的数据转换的内容再现。

[0214] 此外，作为应用存储在信息处理设备中的装置证书和型号 / 版本证书的处理来执行用于检查包括装置、型号和版本的识别信息的设备检查处理。装置证书和型号 / 版本证书用作用于检查使用内容的权利的证书，进行内容管理的管理实体发布装置证书和型号 / 版本证书。

[0215] 参考图 10A 和 10B 说明装置证书和型号 / 版本证书的数据结构的例子。图 10A 示出装置证书的数据结构的例子，图 10B 示出型号 / 版本证书的数据结构的例子。

[0216] 如图 10A 所示，装置证书具有包含装置证书大小、装置证书版本、装置制造商标识符、装置标识符、签名日期、装置公共密钥和电子签名的数据。

[0217] 另一方面，如图 10B 所示，型号 / 版本证书具有包含型号 / 版本证书大小、型号 / 版本证书版本、型号制造商标识符、型号标识符、版本标识符、修改标识符、签名日期、装置公共密钥和电子签名的数据。

[0218] 图 5 所示的安全 VM361 根据从信息记录介质中读出的用于设备检查处理的代码（程序）执行验证装置证书和型号 / 版本证书中的至少一个的处理，检查确认有效性之后的型号、版本和装置中的至少一个，然后进行使用内容代码的处理，例如，根据证实的信息选择用于安全检查的代码或者选择要应用的转换表。

[0219] 例如，作为使用装置证书的具体处理，安全 VM361 首先进行验证装置证书的签名的处理。例如，通过应用作为执行装置证书的签名的实体的管理中心的公共密钥来进行签名验证。作为管理中心的公共密钥，可以应用预先获得、然后存储在设备的存储器中的公共密钥。可选地，可以从信息记录介质或网络获得管理中心的公共密钥。

[0220] 如果通过签名验证没有确认装置证书的有效性，则停止进行包含数据转换的后续内容再现。如果确认了装置证书的有效性，则选择要执行的对应于装置的安全检查代码。可以从装置证书获得装置制造商等基本信息。在以型号或版本为单位进行处理的情况下，执行使用型号 / 版本证书的设备检查处理。

[0221] 安全 VM361 进行验证装置证书和型号 / 版本证书的有效性的处理。如果确认了有效性，则执行获取与信息处理设备或内容使用应用程序相对应的识别信息或属性信息，即来自记录在证书中的信息中的制造商、类型、版本或者设备或应用程序的序列号的处理。根据获得的信息，选择对应于获得的信息的安全检查代码，然后执行基于所选择的代码的安全检查处理。稍后参考流程图说明处理序列的细节。

[0222] 6. 对信息处理设备的加密密钥的分配及内容代码的加密和使用的配置

[0223] 如先前所说明的，安全 VM361 执行基于包含在记录在信息记录介质中的内容代码中的安全检查代码的安全检查处理以及在基于转换表的转换处理中应用的参数计算处理。在该处理中，安全 VM361 根据参考图 1 所说明的设备检查代码 108 执行应用装置证书或型号 / 版本证书的设备检查处理。

[0224] 信息处理设备进行验证装置证书和型号 / 版本证书中的至少一个的有效性的处理。如果确认了有效性，则信息处理设备根据证书的记录信息确定使用信息处理设备或内容的应用程序，选择对应于所确定的信息的安全检查代码，执行基于所选择的代码的安全检查处理，计算在应用转换表 (Fix-up 表) 的数据转换处理中转换内容所需的参数。

[0225] 如上所述，在根据转换表执行的数据替换中，执行应用 (a) 转换数据和 (b) 标识符设置转换数据 (司法标记) 的转换。

[0226] 使用安全检查代码的安全检查或根据转换表执行的数据转换处理是根据基于正确的装置、型号或版本识别信息所选择的内容代码而执行的处理。然而，例如，当未经授权的再现设备从另一个设备复制装置证书或型号 / 版本证书时，可以执行使用未经授权的证书信息的处理。如果仅根据证书的验证确定了对应于信息处理设备的设备类型，即信息处理设备的型号、版本或装置类型，并且执行基于内容代码的安全检查处理或数据转换处理，则可以使用内容而不用进行通常需要的安全检查。此外，原来嵌入内容中的标识符设置转换数据 (司法标记) 可以变为包含不正确的设备信息的数据。即使跟踪嵌入有未经授权的设备信息的内容，也会产生无法跟踪已执行了非法处理的设备的问题。

[0227] 此外，例如，要求非常严格的安全检查的 PC 等信息处理设备 可以复制仅使用宽松的安全检查就可以使用内容的仅用于再现的设备的装置证书，将复制的装置证书存储在 PC 中。然后，在 PC 中，通过应用仅用于再现的设备的装置证书来执行设备检查处理。其结果是，可以通过执行宽松的安全检查来使用内容。

[0228] 因此，如果信息处理设备不提供正确的设备信息（装置、型号和版本中的一个的识别信息），则非法地使用内容，且难以保持对非法使用的跟踪。即，如果提供不正确的设备信息，则不能执行正确的安全检查，不能执行基于转换表的正确的数据转换，不能正确地执行对内容嵌入设备信息（装置、型号和版本中的一个的识别信息）。现在说明防止这种非法行为的配置。

[0229] 即，说明如下配置 :即使当设备提供未经授权的设备信息时，也可以选择对应于每一个设备的正确的内容代码，使得进行与使用内容的信息处理设备或再现应用程序相对应的正常安全检查处理，即使在应用上述转换表的数据转换处理中，也可以执行正确的设备信息的嵌入。

[0230] 在本例子中，为了选择并执行对应于信息处理设备的正确的内容代码，对执行内容再现的多个信息处理设备中的每一个分配根据特定规则的一组特定加密密钥。此外，将记录在信息记录介质中的、由安全 VM 执行的内容代码的至少一部分称为应用了对信息处理设备分配的加密密钥的加密数据。下文中，说明分配加密密钥的配置和处理例子。

[0231] 首先，参考包含图 11 的附图说明存储在信息处理设备中的加密密钥的配置。密钥管理中心对信息处理设备即执行内容再现的信息处理设备分配加密密钥。密钥管理中心将注册信息保持在要分配加密密钥的目的地上。装置标识符、型号标识符和版本标识符对应于信息处理设备。如上所述，将装置标识符设置为每一个信息处理设备特有的标识符。

[0232] 将型号标识符设置为属于同一型号的多个装置（信息处理设备）共有。

[0233] 版本标识符是对属于同一型号的不同版本设置的标识符。例如，假设存在型号 A 的版本 1 和型号 A 的版本 2，则对应于各版本设置独立的版本标识符。

[0234] 密钥管理中心保持并管理信息处理设备的标识符和分配到这些信息处理设备的加密密钥彼此对应的注册表。另一方面，信息处理设备将各种密钥数据或其它证书数据存储在参考图 1 说明的存储器 b161 中，各种密钥数据包括作为装置特有的密钥的装置特有密钥、多个装置的组共有的组密钥、对应于特定设备型号的型号密钥和对应于特定型号的特定版本的版本密钥。密钥管理中心对例如制造商分配该数据，然后，在制造信息处理设备时将其记录在存储器中。

[0235] 图 11 是说明包含密钥管理中心分配到信息处理设备的密钥信息的数据的视图。将密钥管理中心分配到信息处理设备中的每一个的数据大致分为如图 11 所示的三种数据项目。具体地，是 (a) 对应于装置和组的数据、(b) 型号 / 版本包和 (c) 密钥管理中心公共密钥。下文中，说明对应于这些种类的数据。

[0236] (a) 对应于装置和组的数据

[0237] 与制造 LSI 等或再现内容的信息处理设备的装置制造实体相对应地设置具有密钥 [装置制造实体密钥（制造商密钥）] 作为顶点的密钥树。从一个顶点或分支点（节点）开始，设置“N”（在图 11 所示的例子中 n ＝ 256）个最底层密钥。例如，紧接在位于密钥树的顶点的装置制造实体密钥下面的密钥用于对装置制造实体制造并售出的设备或 LSI 按

组进行分类。对组中的每一个设置 G1-1 ～ G1-256 即 256 个不同的组密钥 G1。

[0238] 此外，第三级密钥用于对 G1 层中的每一个进一步进行分类，从而设置 G2-1 ～ G2-256×256 个密钥，即 2562 个不同的组密钥 G2。随后，在第四级，将组 G2 中的每一个进一步分类为设置 2563 个不同的组密钥 G3。此外，在第五级，设置 2 564 个不同的最底层节点（叶片）。对每一个装置分配节点中的每一个，设置对应于每一个装置的装置特有密钥 [Device_Specific_Key]。

[0239] 每一个装置具有：对应于顶层节点的装置制造实体密钥；对应于装置的用作对应于一个最底层节点（叶片）的密钥的装置特有密钥；以及与从对应于装置的叶片到顶层节点的路径上的节点相 对应的密钥，即组密钥（对应于组 G1、G2 和 G3 的密钥）。

[0240] 例如，在图 11 所示的分层结构中，对与最底层叶片相对应的左半部分的装置分配组密钥 G1 501，而不对与最底层叶片相对应的右半部分的装置分配组密钥 G1 501。此外，在图 11 所示的分层结构中，对与最底层叶片相对应的左四分之一的装置分配组密钥 G2 502，而不对与最底层叶片相对应的其它四分之三的装置分配组密钥 G2 502。因此，不同地设置分配到每一个装置的一组加密密钥。此外，每一个装置分配有装置专用密钥 [Device_Key] 以及作为存储有对应于装置的公共密钥的公共密钥证书的装置证书 [Device_Cert]。装置证书具有上述参考图 10A 和 10B 所说明的数据结构。

[0241] 此外，将在图 11 的 (a) 所示的分层结构中相对于顶层节点对叶片设置的密钥称为组密钥和分层密钥或节点密钥。此外，设置层分类的例子仅仅是例子。例如，可以设置为根据许可接受方、平台、销售地区或制造数据进行组分类。

[0242] 作为存储有对应于装置的公共密钥的公共密钥证书的装置证书 [Device_Cert] 存储有装置标识符。每一个播放器具有不同的装置标识符 (ID)。例如，将值 0x00000000 至 0xFFFFFFFF 设置为对应于各装置的装置 ID。

[0243] (b) 型号 / 版本包

[0244] 在信息处理设备中，还存储包含在图 11 的 (b) 所示的型号 / 版本包中的数据。型号 / 版本包包含以下数据。

[0245] (b1) 型号密钥

[0246] (b2) 版本密钥

[0247] (b3) 型号 / 版本专用密钥

[0248] (b4) 型号 / 版本证书

[0249] 型号密钥是对应于信息处理设备的型号特有的密钥数据，版本密钥是对应于信息处理设备的版本特有的密钥数据。型号 / 版本专用密钥和型号 / 版本证书分别对应于在公共密钥加密系统中存储有公共密钥的专用密钥和公共密钥证书。将这些设置为对应于每一个信息处理设备的型号 / 版本特有的密钥信息。型号 / 版本证书存储上述参考图 10 所说明的数据。

[0250] 将型号 / 版本证书配置为与型号 ID ＝ X、版本 ID ＝ Y 以及变形 ID ＝ Z 的代码相对应地设置的证书。

[0251] 如果型号 / 版本证书具有不同的 X、Y 和 Z 的值，则将型号 / 版本证书设置为不同的证书。此外，变形 ID(Z) 是当例如更新固件或再现应用程序而不更新装置的硬件时所更新的代码。当信息处理设备执行该固件更新时，将通过网络或信息记录介质更新的型号 /

版本证书作为更新的结果供给信息处理设备。

[0252] 如上所述，当嵌入识别信息（司法标记）以指定设备时，通过设置型号密钥、版本密钥和型号 / 版本证书以及装置特有密钥和装置证书，可以防止嵌入不正确的识别信息。

[0253] 此外，通过独立地管理与图 11 的 (a) 所示的装置和组以及图 11 的 (b) 所示的型号 / 版本包相对应的数据，例如可以分配制造工厂，从而 LSI 制造商嵌入与根据 LSI 设置有不同的值的装置和组相对应的数据，通过组装 LSI 和其它组件来制造信息处理设备的制造者（组装者）嵌入型号 / 版本包。

[0254] 因此，例如，即使 LSI 是共有的，也可以改变型号或版本。在这种情况下，由于组装者仅需要嵌入嵌入有不同的值的型号密钥等，因此不需要组装者在各设备中嵌入不同的 ID。其结果是，减轻了组装者的负担。此外，即使型号或版本改变，也可以使用已从 LSI 制造商购买的 LSI，而不用调整 LSI。由于该原因，不总是在相同的物理存储器中存储与图 11 的 (a) 所示的装置和组以及图 11 的 (b) 所示的型号 / 版本包相对应的数据，而可以将其存储在独立的存储器中。

[0255] 因此，图 11 的 (a) 中的组密钥（分层密钥，节点密钥）是设置为指定预定装置的分类密钥，而图 11 的 (b) 中的型号密钥和版本密钥是根据所谓的信息处理设备（例如，用于再现光盘的再现设备）的“型号编号”所设置的密钥。这些密钥不需要互相对应。

[0256] (c) 密钥管理中心公共密钥

[0257] 此外，在信息处理设备中除了存储上述 (a) 和 (b) 的数据之外，还存储图 11 的 (c) 所示的密钥管理中心 (KIC) 公共密钥。例如，当信息处理设备验证密钥管理中心授予内容代码的签名时，使用该公共密钥。

[0258] 图 12 示出存储在信息处理设备的存储器中的数据的配置。如图 12 所示，信息处理设备存储有以下数据 (1) ～ (12)。

[0259] (1) 装置制造实体密钥 (Manufacturer Key)

[0260] (2) 第一组密钥 (Group1 Key)

[0261] (3) 第二组密钥 (Group2 Key)

[0262] (4) 第三组密钥 (Group3 Key)

[0263] (5) 装置特有密钥 (Device Specific Key)

[0264] (6) 装置专用密钥 (Device Private Key)

[0265] (7) 型号密钥 #X(Model Key#X)

[0266] (8) 版本密钥 #Y(Version Key#Y)

[0267] (9) 型号 / 版本专用密钥 (Model/Version Private Key)

[0268] (10) 装置证书 (Device Cert)

[0269] (11) 型号 / 版本证书 (MV_CERT(X, Y, Z = Y)(Model/VersionCERT))

[0270] (12) 密钥管理中心公共密钥 (KIC Public Key)

[0271] 在以上数据中，需要非公开地存储除了装置证书、型号 / 版本证书和密钥管理中心公共密钥之外的数据 (1) ～ (9) 以防止数据泄漏，将其存储在安全存储器中。不需要防止装置证书、型号 / 版本证书和密钥管理中心公共密钥的泄漏。

[0272] 图 13 示出说明上述参考图 11 说明的密钥管理中心的数据分配和上述参考图 12 说明的信息处理设备的数据存储之间的相关性的视图。如图 13 所示，将以下数据 (1) ～

(6) 作为对应于装置和组的数据 (a) 存储在安全存储器中。

[0273] (1) 装置制造实体密钥 (Manufacturer Key)

[0274] (2) 第一组密钥 (Group1 Key)

[0275] (3) 第二组密钥 (Group2 Key)

[0276] (4) 第三组密钥 (Group3 Key)

[0277] (5) 装置特有密钥 (Device Specific Key)

[0278] (6) 装置专用密钥 (Device Private Key)

[0279] 此外,将以下数据 (7) ～ (9) 作为包含在型号 / 版本包中的 (b) 数据存储在安全存储器中。

[0280] (7) 型号密钥 #X(Model Key#X)

[0281] (8) 版本密钥 #Y(Version Key#Y)

[0282] (9) 型号 / 版本专用密钥 (Model/Version Private Key)

[0283] 此外,作为不需要在安全存储器中存储的数据,将以下数据 (10) ～ (12) 存储在信息处理设备的存储器中。

[0284] (10) 装置证书 (Device Cert),其包含在对应于装置和组的数据 (a) 中

[0285] (11) 型号 / 版本证书 (MV_CERT(X,Y,Z = Y)(Model/VersionCERT)),其包含在包含在型号 / 版本包中的 (b) 数据中

[0286] (12) 密钥管理中心公共密钥 (KIC Public Key),其包含在 (c) 密钥管理中心公共密钥中

[0287] 最初,将这些密钥和证书信息存储在信息处理设备中以提供给用户。此外,如上所述,例如当更新固件或再现应用程序而不更新装置的硬件时,将已通过网络或信息记录介质更新的型号 / 版本证书作为更新的结果供给信息处理设备。

[0288] 在这种情况下,如图 14 所示,将更新后的型号 / 版本证书通过密钥管理中心或制造商提供给用户的信息处理设备。例如,当将更新后的型号 / 版本证书记录在存储有内容的信息记录介质中时,信息处理设备读出该内容,然后执行在信息处理设备中记录的证书的替换。可选地,例如,可以使用通过网络下载证书而更新的证书来替换证书。

[0289] 通过参考证书内的变形 ID(Z) 来检查型号 / 版本证书是否是更新后的证书 (参考图 10A 和 10B)。例如,每次更新时,变形 ID 增加 (+1)。通过参考变形 ID,可以检查证书的更新状态。

[0290] 例如,在检查使用信息处理设备的型号 / 版本证书的设备的情况下,通过检查存储在信息处理设备的存储器中的型号 / 版本证书来检查更新状态。根据更新状态,可以准确地执行安全检查代码或转换表的选择。

[0291] 制造信息处理设备或设置在信息处理设备中的 LSI 的各种装置制造实体中的每一个可以独立地设置上述参考图 11 和 13 说明的 (a) 对应于装置和组的数据和 (b) 型号 / 版本包等。参考图 15 和 16,说明每一个装置制造实体的密钥数据设置的配置例子。

[0292] 图 15 示出每一个装置制造实体独立地设置 [(a) 对应于装置和组的数据] 的例子。例如,装置制造实体包括 DVD 播放器的制造商、设置在 DVD 播放器中的 LSI 的制造商和再现软件应用程序的制造商。装置制造实体中的每一个定义对应于预定数量的装置的装置 ID,例如 [0x00000000 ～ 0xFFFFFFFF],使装置 ID 对应于树结构叶片,在从叶片到顶点的路

径上设置密钥和证书作为存储在每一个装置中的密钥。如上所述，该路径上的密钥和证书包括以下数据。

[0293] (1) 装置制造实体密钥 (Manufacturer Key)

[0294] (2) 第一组密钥 (Group1 Key)

[0295] (3) 第二组密钥 (Group2 Key)

[0296] (4) 第三组密钥 (Group3 Key)

[0297] (5) 装置特有密钥 (Device Specific Key)

[0298] (6) 装置专用密钥 (Device Private Key)

[0299] (7) 装置证书 (Device Cert)

[0300] 图 1 5 示出装置制造实体 (制造商)1 ～ N。“N”个装置制造实体中的每一个可以设置上述 (1) 装置制造实体密钥 (ManufacturerKey) ～ (7) 装置证书 (Device Cert) 的数据作为存储在信息处理设备中的数据。在这种情况下，在信息处理设备中，以与作为设备的制造实体所注册的设置数量相同的数量将 (1) 装置制造实体密钥 (Manufacturer Key) ～ (7) 装置证书 (Device Cert) 的数据存储在存储器中。

[0301] 类似地，每一个装置制造实体还可以独立地设置 [(b) 型号 / 版本包]。图 16 示出装置制造实体 (制造商)1 ～ N。如图 16 所示，“N”个装置制造实体中的每一个可以设置 [(b) 型号 / 版本包] 作为存储在信息处理设备中的数据。

[0302] 如上所述，(b) 型号 / 版本包包括以下数据。

[0303] (1) 型号密钥 #X(Model Key#X)

[0304] (2) 版本密钥 #Y(Version Key#Y)

[0305] (3) 型号 / 版本专用密钥 (Model/Version Private Key)

[0306] (4) 型号 / 版本证书 (MV_CERT(X, Y, Z ＝ Y)(Model/VersionCERT))

[0307] 此外，每一个装置制造实体独立地设置包含上述数据的包。

[0308] 如图 16 中的装置制造实体 (制造商 1) 所示，每一个装置制造实体 (Manufacturer) 设置根据装置制造实体所制造的装置的型号 (X) 和版本 (Y) 而不同的型号 / 版本包。存储在信息处理设备中的包用作对应于信息处理设备的型号 / 版本的包数据。

[0309] 此外，可以将包括信息处理设备的组装者所提供的型号 / 版本包和设置在信息处理设备中的 LSI 的制造商所提供的型号 / 版本包的多个型号 / 版本包存储在信息处理设备中。即，在信息处理设备中，将与信息处理设备的制造商、组件制造商或组装者等多个不同的装置制造实体相对应的一组独立密钥存储在存储器中。在解密内容代码时，用作信息处理设备的数据处理单元的安全 VM 从对应于与所执行的内容代码相对应地选择的装置制造实体的密钥集中选择密钥，然后应用所选择的密钥对包含在内容代码中的数据执行解密处理。

[0310] 此外，密钥管理中心产生密钥数据或证书数据，将其提供给装置制造实体。参考图 17，现在说明在密钥管理中心中产生密钥数据和证书数据的处理。图 17 示出 (a)、(b1) 和 (b2) 所示的产生数据的三种例子。

[0311] 图 17 的 (a) 示出对应于装置和组产生数据的例子。首先，密钥管理中心通过利用例如随机数产生处理产生与要制造的装置的数量相对应的装置特有数据，然后使数据产生单元 521 执行以该装置特有数据作为输入值的数据处理，从而产生装置特有密钥并产生

包含装置证书和装置专有密钥的[(a)对应于装置和组的数据]。

[0312] (b1)示出产生(b)型号/版本包的例子。首先,密钥管理中心通过利用例如随机数产生处理产生与要产生的型号/版本的数量相对应的特有数据,然后使数据产生单元522执行以该特有数据作为输入值的数据处理,从而产生包含型号密钥、版本密钥和型号/版本证书的[(b)型号/版本包]。

[0313] (b2)示出产生包含在(b)型号/版本包中的型号/版本证书的更新后的数据的例子。首先,密钥管理中心通过利用例如随机数产生处理来产生与更新后的型号/版本相对应的特有数据,然后使数据产生单元523执行以该特有数据作为输入值的数据处理,从而产生更新后的型号/版本证书。此外,更新后的型号/版本证书具有记录通过使记录有更新后的型号/版本证书的变形ID在更新前增加"1"而获得的变形ID的数据结构。通过网络或盘(disc)等信息记录介质向作为用户设备的信息处理设备提供更新后的型号/版本证书,从而用更新后的型号/版本证书替换已存储在信息处理设备中的更新前的型号/版本证书。

[0314] 首先,如先前参考图1等所说明的,将包含密钥管理中心分配到信息处理设备的密钥信息的数据组大致划分为以下三种(a)～(c)。

[0315] (a)对应于装置和组的数据

[0316] (b)型号/版本包

[0317] (c)密钥管理中心公共密钥

[0318] 在(a)～(c)中,(c)密钥管理中心公共密钥应用于验证授予内容代码的电子签名。即,(c)密钥管理中心公共密钥用于验证存储在信息记录介质中的内容代码是否是未变更的授权代码。

[0319] 参考图18说明对内容代码设置电子签名的例子。密钥管理中心(KIC)执行图18所示的步骤S201的处理。密钥管理中心(KIC)输 入包含设备检查代码、安全检查代码或包含转换表的处理代码等各种内容代码的文件[000xx.svm]。这些代码是内容提供商或装置制造实体等各种实体所产生的文件。密钥管理中心(KIC)输入内容代码文件,验证该内容代码文件,对文件中的每一个产生并输出应用密钥管理中心(KIC)的专用密钥的签名。在输出中,对内容代码文件中的每一个设置签名[Sig]。

[0320] 在信息处理设备从信息记录介质中读出内容代码并执行各种处理的情况下,信息处理设备首先执行验证授予所读取的内容代码文件的电子签名的处理。应用密钥管理中心公共密钥执行该处理。仅当通过验证确认该内容代码是未变更的授权代码时,执行应用包含在该文件中的内容代码的处理。

[0321] 可以已各种方式设置签名的授予。参考图19说明授予签名的例子。图19示出对内容代码文件[00000.svm]设置签名的例子。作为输入的内容代码文件是内容提供商或装置制造实体等各种实体产生的文件。预先将该文件划分为以2MB为数据单位的块。此外,对于以2MB为数据单位的块中的每一个,将空数据(dummy data)记录在文件中作为存储签名的区域。

[0322] 密钥管理中心(KIC)输入包含空数据的内容代码文件,每2MB的数据地验证内容代码文件,对2MB的块中的每一个产生并输出应用了密钥管理中心(KIC)的专用密钥的签名。

[0323] 在信息处理设备从信息记录介质中读出内容代码并执行各种处理的情况下，信息处理设备首先执行验证授予使用所读取的内容代码文件的区域的电子签名的处理。应用密钥管理中心公共密钥执行该处理。仅当通过验证确认属于使用该内容代码文件的区域的数据是未变更的授权代码时，执行应用包含在该文件区域中的内容代码的处理。

[0324] 参考图 20 说明读取内容代码文件的特定数据区域和在信息处 理设备中执行的签名验证处理的具体例子。图 20 的 (1) 示出存储在信息记录介质中的内容代码。这里，示出两个内容代码文件 [AAAAA.svm] 和 [BBBBB.svm]。

[0325] 图 20 的 (2) 示出设置为能够读出信息记录介质的信息处理设备内的存储区域，具体地，可以使用上述参考图 1 所说明的安全 VM160 的 VM 存储区域作为存储空间。安全 VM 执行内容代码处理。当从信息记录介质中读出指定内容代码的特定区域时，安全 VM 使用 (CALL_LoadContentCode) 作为内容代码文件数据的读取命令的执行函数，这是预定义代码读取命令。

[0326] 内容代码文件数据的读取命令 (CALL_LoadContentCode) 例如是包含以下指定信息的命令。

[0327] UINT8 conte ntcode[5] :内容代码文件编号 (= AAAAA)

[0328] UINIT32 block :内容代码文件内的块编号 = 2

[0329] UINT32 Offset :开始加载块内内容代码的位置

[0330] UINT32 len :所加载的内容代码的文件长度

[0331] UINT8 *dstPtr :加载目的地的 VM 存储地址

[0332] 使用包含指定信息的内容代码文件数据的读取命令的执行函数 (CALL_Load Content Code)，将位于预定内容代码文件的预定区域中的数据加载到 VM 存储区域中。

[0333] 此外，在加载时，执行签名验证。例如，加载内容代码文件 [AAAAA.svm] 的第二块时的具体处理序列如下。

[0334] (步骤 1) 访问 AAAAA.svm 文件的第二块的头

[0335] (步骤 2) 进行访问块的签名验证

[0336] (步骤 3) 从与块体的偏移字节相对应的位置开始加载所加载的内容代码文件长度 (len) 字节，然后将其复制到从 VM 存储地址 (*dstPtr) 开始的 VM 存储区域的空间

[0337] 通过该处理步骤，执行签名验证和数据加载。此外，如果签名验证判断为可能存在数据变更，则不进行加载处理和使用内容代码的处理。

[0338] 接下来，参考图 21，说明存储在信息记录介质中的内容代码的加密。首先，如先前参考图 9 所说明的，将内容代码文件分为以下四种 (a) ～ (d)。

[0339] (a) 全部内容和全部装置共有的内容代码

[0340] (b) 内容特有的内容代码

[0341] (c) 装置、型号或版本特有的内容代码

[0342] (d) 内容和设备特有的内容代码 (例如，装置、型号或版本)

[0343] 将每一个内容代码作为独立的文件存储在信息记录介质中，或者将整个内容代码作为一个文件存储在信息记录介质中。产生属于各种类的内容代码的实体可以不同。例如，作为内容生产商的工作室设置对应于 (b) 内容特有数据的内容代码。此外，制造再现设备或再现应用程序的实体在很多情况下产生 (c) 装置、型号或版本等特有数据。

[0344] 因此，参考图 21 说明直到将不同的实体产生的内容代码存储在信息记录介质中为止的序列。参考图 21，[00000.svm] ～ [00003.svm] 表示不同的实体，即生产并编辑内容的工作室、制作公司以及设备或再现应用程序的制造商或者在信息处理设备中设置的 LSI 等组件的制造商所产生的内容代码文件 551。

[0345] 这些内容代码文件 [00000.svm] ～ [00003.svm] 具有假设使用型号 / 版本 / 装置特有的密钥，即上述参考图 11 ～ 13 已说明的节点密钥（组密钥 [Gn] 或装置特有密钥）、型号密钥或版本密钥对内容代码的一部分进行加密而制备的内容代码。

[0346] 此外，产生内容代码文件 [00000.svm] ～ [00003.svm] 的实体产生具有内容代码的加密配置信息的内容代码加密配置信息 552，然后将内容代码加密配置信息 552 和产生的内容代码发送到密钥管理中心。如图 21 所示，内容代码加密配置信息 552 包括对应于作为内容代码识别信息的内容代码编号的数据、加密段信息和应用于加密段的密钥的指定信息。

[0347] 在密钥管理中心中，对从各内容代码产生实体接收到的内容代码执行基于内容代码加密配置信息 552 的加密。即，密钥管理中心选择根据内容代码加密配置信息 552 指定的装置制造实体密钥、组密钥 [Gn] 或装置特有密钥或者型号密钥或版本密钥等密钥，对根据内容代码加密配置信息 552 所指定的内容代码的指定部分进行加密。

[0348] 因此，产生图 21 所示的加密完成内容代码 553。将加密完成内容代码 553 发送到作为信息记录介质制造实体的盘工厂，然后将其记录在盘中。此外，还将内容代码加密配置信息 552 发送到盘工厂，然后将其记录在盘中。此外，可以将内容代码加密配置信息 552 包含在形成内容代码的数据中，从而将其记录在信息记录介质中，或者在信息记录介质中作为特有的独立文件进行记录。

[0349] 图 21 示出作为加密完成内容代码 553 的四个内容代码文件 [00000.svm] ～ [00003.svm]。该内容代码中的每一个包含部分加密的加密数据。例如，加密所应用的加密密钥是装置制造实体密钥、组密钥 [Gn] 或装置特有密钥或者型号密钥或版本密钥，应用根据内容代码加密配置信息 552 所选择的密钥执行加密。

[0350] 例如，假设应用图 11 的 (a) 所示的组密钥 G1 501 加密了内容代码文件 00000.svm，仅持有组密钥 G1 501 的装置可以解密该加密数据。因此，仅与对应于图 11 所示的分层结构中的最底层叶片的左半部分的装置相对应的装置可以使用内容代码 00000.svm 的加密数据。因为对应于最底层叶片的右半部分的装置未持有组密钥 G1 501，所以不能使用内容代码 000 00.svm 的加密数据。

[0351] 以相同的方式，例如，假设应用图 11 的 (a) 所示的组密钥 G2502 加密了内容代码文件 00001.svm，仅持有组密钥 G2 502 的装置可以解密该加密数据。因此，仅与图 11 所示的分层结构中的最底层叶片相对应的左四分之一的装置可以使用内容代码 00001.svm 的加密数据。

[0352] 因此，因为应用组密钥 Gn 或装置特有密钥、型号密钥或版本密钥加密了内容代码，所以可以限制能够解密并使用内容代码的装置数量。如上所述，内容代码包括用于安全检查的安全检查代码和应用于内容的数据转换的转换表。此外，可以设置为仅对特定装置执行安全检查处理或数据转换处理。

[0353] 因此，在应用例如通过从其它装置复制装置证书或型号 / 版本证书而获得的未经

授权的证书执行设备检查的情况下，因为内容代码包括仅可以用存储在证书所证明的信息处理设备中的密钥进行解密的数据，所以即使获得了对应于装置信息等的特定内容代码以执行设备检查处理，也不可以解密内容代码。即，即使执行了应用借用的证书的设备检查，信息处理设备也不包含对应于该证书的密钥，即装置制造实体密钥、组密钥 Gn 或装置特有密钥、型号密钥或版本密钥，因此，不能解密该内容代码。其结果是，可以防止非法应用与未经授权的证书所指定的设备信息相对应的特定内容代码。

[0354] 接下来，参考图 22 说明信息处理设备执行的内容代码处理。执行内容再现的信息处理设备的数据处理的安全 VM 获取包含记录在信息记录介质中的数据处理程序的内容代码，根据该内容代码执行数据处理。如前所述，应用装置制造实体密钥、组密钥 Gn 或装置特有密钥、型号密钥和版本密钥中的任意一个加密内容代码中的至少一部分。

[0355] 安全 VM 获取应用于解密内容代码的密钥指定信息和表示在 来自存储在信息记录介质中的数据中的内容代码中设置的加密数据的位置的加密数据位置指定信息，根据获得的信息从存储器中选择要应用的密钥，根据加密数据位置指定信息指定要解密的数据，应用所选择的密钥执行解密。

[0356] 图 22 是示出安全 VM652 执行的处理的视图。安全 VM652 读出存储在信息记录介质中的内容代码，然后进行处理。安全 VM652 通过将从信息记录介质读出的内容代码存储在安全 VM 的存储器 651 中来执行该处理。

[0357] 此外，在装置存储密钥 650 中，示出密钥管理中心 (KIC) 所分配的上述参考图 11 ～ 13 说明的密钥，即装置制造实体密钥、组密钥 Gn 或装置特有密钥、型号密钥、版本密钥、装置证书和型号 / 版本证书。

[0358] 首先，在步骤 S251 中，安全 VM652 从存储在安全 VM 的存储器 651 中的存储器存储数据 661 中获取在要处理的内容代码中设置的加密密钥数据 [X]662。然后，安全 VM652 根据从包含在内容代码或其它数据文件中的记录数据中获得的密钥指定信息从播放器存储密钥 650 中选择应用于对加密密钥数据 [X]662 进行解密的密钥。密钥指定信息是根据上述参考图 21 所说明的内容代码加密配置信息 552 记录在信息记录介质中的信息。

[0359] 在本例子中，假设密钥指定信息是用于指定密钥 ID ＝ 4 即装置特有密钥 (Device_Specific_Key) 的信息。安全 VM652 根据密钥指定信息 [密钥 ID ＝ 4] 从装置存储密钥 650 中选择装置特有密钥 (Device_Specific_Key)，对加密密钥数据 [X]662 执行解密处理。

[0360] 解密处理的结果是，获得通过加密一部分内容代码而获得的原始加密密钥 [K]。然后，在步骤 S252 中，安全 VM652 应用获得的原始加密密钥 [K] 解密对应于内容代码的加密部分的输入数据 663，将解密的结果作为输出数据 664 存储在安全 VM 的存储器 651 中。由于该处理，信息处理设备可以使用例如装置特有的内容代码。

[0361] 此外，通过对于安全 VM 执行内容再现处理的再现 (播放器) 应用程序的中断 (INTRP) 序列以及对于再现 (播放器) 应用程序的安全 VM 的应答 (呼叫) 处理，执行安全 VM652 中的处理。例如通过调用以下函数来执行内容代码的解密处理。

[0362] CALL_AES(输出目的地地址，输入数据地址，AES 处理块数，密钥地址，密钥 ID)

[0363] 该函数用于使得通过使用密钥 ID(图 22 中的 ID ＝ 4) 指定的播放器持有的专用密钥对密钥地址所指定的 128 位的值 (图 22 中的加密密钥数据 [X]662) 进行解密，用于使得通过使用解密的结果作为解密密钥对与从输入数据地址开始的 AES 处理块数 ×16 字节

相对应的数据进行解密，用于使得将解密后的数据输出到输出目的地地址。如上所述，使用装置特有密钥嵌入识别信息。因此，即使第一装置尝试嵌入第二装置的识别信息，第一装置也不能获得第二装置的Device_specific_Key，因此，不能解密第二装置的数据。其结果是，因为不能指定另一个装置的识别信息，可以可靠地指定预定装置。

[0364] 接下来，参考图 23 说明信息处理设备执行的另一个内容代码处理。图 23 是说明应用装置存储密钥 650 中的装置专用密钥 [Device_Private_Key] 的签名处理的视图。

[0365] 在步骤 S272 中，安全 VM652 例如应用 SHA-1 等 Hash（哈希）函数计算存储在安全 VM 的存储器 651 中的存储器存储数据 671 的输入数据 672 的 Hash 值。此外，在作为计算 Hash 值之前的步骤的步骤 S271 中，可以增加播放器信息或媒体信息。然后，在步骤 S273 中，从装置存储密钥 650 中获得装置专用密钥 [Device_Private_Key]，关于 Hash 值的电子签名，例如执行基于 EC-DSA 算法的电子签名，将包含签名的数据作为输出数据 673 存储在安全 VM 的存储器 651 中。之后，获得输出数据 673，然后在执行内容代码时执行签名验证，因此，可以验证信息处理设备的有效性。在上述说明中，即使将 [Device_Private_Key] 设置为 EC-DSA 的密钥，也可以通过将 [Device_Private_Key] 设置为 RSA 的密钥来授予 RSA 签名。

[0366] 此外，例如，当安全 VM652 调用以下函数时，执行签名设置处理。

[0367] CALL_Private_Key（输出目的地地址，输入数据地址，要签名的数据的长度，选项指定，密钥 ID）

[0368] 该函数用于使得从输入数据地址中提取对应于要签名的数据长度的数据，用于使得通过使用 SHA-1 函数将以字节行增加的选项指定媒体 / 播放器信息转换为 Hash 值，用于使得将装置自己的专用密钥签名为转换结果，然后记录在输出目的地地址中。

[0369] 如上所述，在使用存储在信息记录介质中的内容的信息处理设备中，除了存储上述参考图 11 ～ 13 说明的密钥管理中心 (KIC) 分配的装置制造实体密钥、组密钥 Gn、装置特有密钥、型号密钥、版本密钥、装置证书和型号 / 版本证书之外，还存储密钥数据和证书数据。信息处理设备使用内容代码，通过选择性地应用这些密钥的加密处理来设置签名。因为将包含通过所选择的特有密钥加密的数据部分的内容代码存储在信息记录介质中，仅存储所选择的特有密钥的特定设备可以使用内容代码。

[0370] 接下来，参考图 24 和 25 说明在信息处理设备中使用内容代码的处理序列。图 24 是说明应用装置证书 (Device Cert) 和型号 / 版本证书 (MV Cert) 的设备检查处理的序列的流程图，图 25 是说明通过选择对应于型号 / 版本的转换表 (Fix_up 表) 和安全检查代码所执行的序列的流程图。图 24 和 25 中的两个流程图是图 1 所示的安全 VM 160 所执行的处理，通过读出存储在信息记录介质中的内容代码来执行该处理。

[0371] 作为应用包含在内容代码中的设备检查代码的处理来执行图 24 所示的设备检查处理。用于设备检查处理的代码包括以下函数，安全 VM 执行该代码。

[0372] [Call_Discovery]

[0373] [Call_PrivateKey]

[0374] 函数 [Call_Discovery] 用于使得从信息处理设备内的存储器中获取装置证书或型号 / 版本证书，以执行签名验证处理。

[0375] 此外，如上所述，[Call_Private_Key] 函数用于使得从输入数据地址中提取与要

签名的数据的长度相对应的数据，使得用装置自己的专用密钥签名以将其记录在输出目的地地址中。

[0376] 接下来，根据图 24 中的流程说明信息处理设备执行的设备检查处理的过程。首先，在步骤 S301 中，开始内容代码处理（这里，是设备检查处理）。然后，在步骤 S302 中，安全 VM 判断在设备检查处理执行代码中是否包含使得执行调用及验证装置证书的处理的函数 [Call_Discovery]。如果判断为包含使得执行调用及验证装置证书的处理的函数 [Call_Discovery]，则执行函数 [Call_Discovery]。然后，在步骤 S303 中，从信息处理设备的存储器中获取装置证书 (Device Cert)。如果判断为不包含使得执行调用及验证装置证书的处理的函数 [Call_Discovery]，则该处理进行到步骤 S308。

[0377] 在步骤 S303 中从信息处理设备的存储器中获得装置证书 (Device Cert) 之后，在步骤 S304 中，作为应用存储在信息处理设备的存储器中的密钥管理中心的公共密钥的签名验证处理来执行验证在装置证书 (Device Cert) 中设置的签名的处理。如果通过签名验证没有确认装置证书的有效性，则该处理停止。

[0378] 在步骤 S303 中，如果通过签名验证确认了装置证书的有效性，则该处理进行到步骤 S305。在步骤 S305 中，执行包含在内容代码中的函数 [Call_PrivateKey]。即，使用信息处理设备的装置专用密钥执行对信息处理设备产生的随机数或从信息记录介质读取的数据的签名处理。然后，在步骤 S306 中，验证产生的签名。通过应用从确认了有效性的装置证书获得的装置公共密钥来执行验证。

[0379] 如果签名验证未成功，则判断为信息处理设备没有对应于从装置证书获得的装置公共密钥的正确的装置专用密钥，因此，该处理停止。如果签名验证成功，则该处理进行到步骤 S307。在步骤 S307 中，确定信息处理设备具有对应于从装置证书获得的装置公共密钥的正确的装置专用密钥。即，确定该信息处理设备是有效的信息处理设备。因此，从装置证书获取装置标识符（装置 ID），从而确定了对应于该信息处理设备的装置 ID。

[0380] 然后，在步骤 S308 中，安全 VM 判断在设备检查处理执行代码中是否包含使得执行调用及验证型号 / 版本证书的处理的函数 [Call_Discovery]。如果判断为包含使得执行调用及验证型号 / 版本证书的处理的函数 [Call_Discovery]，则执行函数 [Call_Discovery]。然后，在步骤 S310 中，从信息处理设备的存储器中获取型号 / 版本证书 (MV Cert)。如果判断为不包含使得执行调用及验证型号 / 版本证书的处理的函数 [Call_Discovery]，则判断为已完成常规设备检查处理，完成该处理。

[0381] 在步骤 S309 中从信息处理设备的存储器中获得型号 / 版本证书 (MV Cert) 之后，在步骤 S310 中，作为应用存储在信息处理设备的存储器中的密钥管理中心的公共密钥的签名验证处理来执行验证在型号 / 版本证书 (MV Cert) 中设置的签名的处理。通过签名验证，如果没有确认型号 / 版本证书的有效性，则该处理停止。

[0382] 在步骤 S310 中，如果通过签名验证确认了型号 / 版本证书的有效性，则该处理进行到步骤 S311。在步骤 S311 中，执行包含在内容代码中的函数 [Call_PrivateKey]。即，使用信息处理设备的型号 / 版本专用密钥执行对信息处理设备产生的随机数或从信息记录介质读取的数据的签名处理。然后，在步骤 S312 中，验证产生的签名。通过应用从确认了有效性的型号 / 版本证书获得的型号 / 版本公共密钥来执行验证。

[0383] 如果签名验证未成功，则确定信息处理设备没有对应于从型号 / 版本证书获得的

型号/版本公共密钥的正确的型号/版本专用密钥，因此，该处理停止。如果签名验证成功，则该处理进行到步骤S313。在步骤S313中，确定信息处理设备具有对应于从型号/版本证书获得的型号/版本公共密钥的正确的型号/版本专用密钥。即，确定该信息处理设备是有效的信息处理设备。因此，从型号/版本证书获取型号/版本标识符（型号/版本ID），从而确定了对应于该信息处理设备的型号ID或版本ID。

[0384] 因此，信息处理设备应用装置证书和型号/版本证书或装置专用密钥或型号密钥/版本密钥中的至少一个来执行设备检查处理。该处理的结果是，指定设备的装置ID、型号ID和版本ID中的至少一个。即，通过使用对应于每一个装置的特有密钥或型号或版本共有的密钥以及电子证书，可以可靠地指定信息处理设备。

[0385] 接下来，参考图25中的流程图，说明通过选择对应于型号/版本的转换表(Fix_up表）和安全检查代码所执行的序列。

[0386] 该处理也是图1所示的安全VM160执行的处理，通过读出存储在信息记录介质中的内容代码来执行该处理。作为应用包含在内容代码中的转换表(Fix_up表）和安全检查代码的处理来执行该处理。

[0387] 首先，在步骤S321中，判断在记录在信息记录介质中的内容 代码中是否包含与在上述参考图2 4说明的设备检查处理中指定的型号ID、版本ID和装置ID中的至少一个相对应的安全检查代码（固有代码）。如果判断为不包含该安全检查代码，则省略安全检查，进行到步骤S324。

[0388] 如果在记录在信息记录介质中的内容代码中包含与在设备检查处理中指定的型号ID、版本ID和装置ID中的至少一个相对应的安全检查代码（固有代码），则该处理进行到步骤S322。在步骤S322中，执行与型号ID、版本ID或装置ID相对应的安全检查代码（固有代码）。此外，当执行该代码时，通过签名验证来检查该代码的有效性。仅当确认了有效性时，执行该处理。此外，使用所选择的密钥，即，装置制造实体密钥、组密钥Gn或装置特有密钥、型号密钥或版本密钥来加密该代码的至少一部分。在这种情况下，首先，根据上述参考图21说明的内容代码加密配置信息552的密钥指定信息，需要通过从存储器获取相应的密钥来执行解密处理。

[0389] 在很多情况下，设备所需的安全代码是型号/版本共有的代码。因此，对于执行安全代码，即使未指定装置ID(即，即使不执行图24的步骤S302～S307)，通过进行图24的处理S308～S313也可以可靠地指定型号。因此，不特别需要指定装置ID的处理。

[0390] 另一方面，在发布非法复制的内容、因此嵌入在非法副本中的识别数据已指定了在特定非法副本中使用的装置时的情况下，将通过网络获取的或记录在记录介质中的内容代码配置为与装置ID的指定相对应的已在非法副本中使用的一个装置特有的内容代码。即，即使在型号相同的情况下，对一个特定的装置执行特定的处理，而不执行内容代码。

[0391] 如果在步骤S323中完成了常规的安全检查，则该处理进行到步骤S324。如果未完成常规的安全检查，则不允许使用内容代码，停止该处理。

[0392] 在步骤S324中，开始再现内容。在再现内容时，首先，根据上述参考图5说明的处理序列来执行使用对应于内容的标题密钥的解密处理。然后，在步骤S325中，选择对应于指定的型号ID、版本ID和装置ID中的至少一个的转换表(Fix_up_table)以执行内容数据的转换（媒体变换）。然后，在步骤S326中，将转换完成内容数据例如输出到显示装置以执

行内容再现。

[0393] 在应用转换表（Fix_up 表）的内容数据转换（媒体变换）中，包含将内容数据转换为包含在内容中的正常数据的处理以及将对应于信息处理设备的识别信息嵌入包含在内容中的部分数据中的处理。此外，对于嵌入对应于信息处理设备的识别信息，指定装置 ID 并嵌入对应于装置 ID 的数据即可。即，不需要指定型号。例如，当不包含对应于型号 / 版本的安全代码时，通过将内容代码记录在记录介质中、通过仅执行装置 ID 指定处理获得内容代码（例如，图 24 的步骤 S302 ～ S307）并省略型号 / 版本指定处理（例如，图 24 的步骤 S308 ～ S313），可以快速地执行嵌入识别信息的处理。

[0394] 7. 信息处理设备的配置

[0395] 接下来，参考图 26，说明应用再现（播放器）应用程序和安全 VM 的数据处理的信息处理设备的硬件配置的例子。信息处理设备 80 包括 :CPU809，其执行根据 OS 或内容的再现或记录应用程序的各种处理、相互验证处理和内容再现，即，执行包含上述根据内容代码的设备检查处理、基于安全检查代码的安全检查处理和应用转换表的数据转换处理的各种程序的多种数据处理 ；用作存储程序、参数等的区域的 ROM808 ；存储器 810 ；输入、输出数字信号的输入输出 I/F802 ；输入、输出模拟信号并具有 A/D、D/A 转换器 805 的输入输出 I/F804 ；执行 MPEG 数据的编码、解码的 MPEG CODEC 803 ；执行 TS（传输流）和 PS（程序流，programstream）处理的 TS 和 PS 处理单元 806 ；执行包含相互验证的多种代 码处理和对加密内容的解密处理的代码处理单元 807 ；硬盘等记录介质 812 ；执行数据记录和再现信号的输入、输出的驱动 811，每一个块都连接到总线 801。

[0396] 信息处理设备（主机）800 通过 ATAPI-BUS 连接总线连接到驱动。通过数字信号输入输出 I/F802 输入、输出转换表、内容等。代码处理单元 807 例如应用 AES 算法来执行加密处理和解密处理。

[0397] 此外，例如，将执行内容再现或记录处理的程序存储在 ROM808 中。在执行程序时，存储器 810 根据需要用作工作区或参数和数据的存储区。例如，ROM808 或记录介质存储有上述多种密钥数据或证书数据。

[0398] 当再现内容或将内容输出到外部时，应用从信息记录介质获得的数据转换处理程序执行解密加密的内容、恢复转换表或根据存储在转换表中的数据记录转换数据的处理等根据上述处理序列的处理。

[0399] 8. 信息记录介质制造设备和信息记录介质

[0400] 接下来，说明信息记录介质制造设备和信息记录介质。即，说明用于制造在上述内容再现处理中应用的信息记录介质的设备和方法以及信息记录介质。

[0401] 信息记录介质制造设备是制造存储有例如上述参考图 1 所说明的记录数据的信息记录介质 100 的设备。在信息记录介质 100 中，存储包含设备检查代码和安全检查代码或转换表的内容代码。如上述参考图 21 所说明的，用各种所选择的密钥对内容代码的至少一部分进行加密。

[0402] 如图 27 所示，信息记录介质制造设备包括 :内容文件产生单元 901，其产生存储有记录在信息记录介质中的内容数据的内容文件 ；内容代码文件产生单元 902，其产生用于使用内容时所执行的设备检查处理的内容代码、包含用于安全检查处理的程序的内容 代码以及存储有应用于内容的数据转换的转换表的内容代码文件 ；以及记录单元 903，其在

信息记录介质910中记录在内容文件产生单元901中产生的内容文件和在内容代码文件产生单元902中产生的内容代码文件。

[0403] 内容代码文件产生单元902产生存储有用于执行用于存储在每一个信息处理设备的存储器中的设备证书的设备检查处理的设备检查代码的内容代码文件、存储有可以根据设备检查处理所检查的设备标识符选择性地执行的安全检查代码的内容代码文件、以及存储有在可以根据设备检查处理所检查的设备标识符选择性地执行的内容的数据转换处理中应用的数据转换表的内容代码文件。

[0404] 内容代码文件产生单元902用于产生存储有包含仅使用分配到使用内容的信息处理设备组的加密密钥可以解密的加密数据的内容代码的内容代码文件。在这种情况下，在具有上述参考图11～13所说明的分层结构的密钥树中，作为加密密钥应用包含与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应地设置的型号密钥和与信息处理设备的版本相对应地设置的版本密钥的加密密钥中的一个。

[0405] 此外，作为与存储有包含仅使用分配到使用内容的信息处理设备的特定组的加密密钥可以解密的加密数据的内容代码的内容代码文件相对应的信息，内容代码文件产生单元902执行产生上述参考图21所说明的内容代码加密配置信息，即作为要在信息记录介质中记录的信息的包含密钥指定信息和内容代码的加密数据部分的内容代码加密配置信息的处理。

[0406] 在信息记录介质制造设备制造的信息记录介质910中，记录参 考图1等所说明的多种数据。具体地，至少包含存储有内容数据的内容文件、存储有包含用于当使用内容时所执行的设备检查处理的内容代码中的至少一个的内容代码的内容代码文件、用于安全检查处理的程序以及在包含在存储在信息记录介质中的内容中的数据的数据转换处理中应用的数据产生处理代码。

[0407] 记录在信息记录介质910中的内容代码文件包括存储有包含仅使用分配到使用内容的信息处理设备的特定组的加密密钥可以解密的加密数据的内容代码的内容代码文件。在这种情况下，在具有上述参考图11～13所说明的分层结构的密钥树中，作为加密密钥应用包含与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体密钥、与信息处理设备的型号相对应地设置的型号密钥和与信息处理设备的版本相对应地设置的版本密钥的加密密钥中的一个。

[0408] 此外，作为与存储有包含仅使用分配到使用内容的信息处理设备的特定组的加密密钥可以解密的加密数据的内容代码的内容代码文件相对应的信息，在信息记录介质910中记录上述参考图21所说明的内容代码加密配置信息，即包含密钥指定信息和内容代码的加密数据部分的内容代码加密配置信息。

[0409] 在上文中，参考特定实施例详细说明了本发明。然而，明显可知，本领域技术人员可以对实施例进行各种变化和变形，而不脱离本发明的精神或范围。即，应当理解，上述实施例不是限制性的，而是说明性的。为了确定本发明的精神或范围，应当参考所附权利要求。

[0410] 此外，可以用硬件、软件或硬件和软件二者的合成配置来执行在说明书中说明的处理。在使用软件执行该处理的情况下，可 以将记录有处理序列的程序安装在置于专用硬件中的计算机内的存储器中以执行该程序，或者可以将该程序安装在能够执行多种处理的通用计算机中以执行该程序。

[0411] 例如，可以预先在用作记录介质的硬盘或ROM（只读存储器，read only memory）中记录程序。可选地，可以将程序临时或持久地存储（记录）在包含软盘、CD-ROM（光盘只读存储器，compactdisc read only memory）、MO（磁光，magneto optical）盘、DVD（数字通用盘，digital versatile disc）、磁盘和半导体存储器的可移动存储介质中。可以作为所谓的包软件（packa ge software）提供该可移动存储介质。

[0412] 可选地，除了将来自可移动存储介质的程序安装在计算机中之外，还可以通过LAN（局域网，local area network）或因特网等网络将程序无线地发送到计算机或者有线地发送到计算机。然后，计算机可以接收无线地发送或者有线地发送的程序，然后将该程序安装在设置在计算机中的硬盘等记录介质中。

[0413] 此外，不仅能够以时序的方式而且能够以并行、或者根据执行处理的设备的处理性能或根据需要独立地执行在说明书中说明的多种处理。此外，在说明书中，系统是多个装置的逻辑组。即，其不限于同一机壳中现有的装置。

[0414] 此外，在签名中使用的公共密钥或专用密钥可以基于使用所谓的RSA的方法或者使用所谓的椭圆代码（ellipticalcode）（EC-DSA）的方法。

[0415] 如上所述，根据本发明实施例的配置，在获取包含记录在信息记录介质中的数据处理程序的内容代码、然后执行安全检查处理、对包含在内容中的数据的转换处理或根据相应的内容代码将设备信息嵌入内容的处理等数据处理的配置中，作为检查信息处理设备的处理来执行应用存储在信息处理设备中的装置证书或型 号／版本证书的设备检查处理，在设备检查处理之后获取用作记录在装置证书或型号／版本证书中的设备标识符的装置ID、型号ID或版本ID，在应用内容代码进行处理时，执行应用对应于获得的设备标识符的内容代码的数据处理。其结果是，可以选择并应用对应于每一个设备的适当的内容代码。

[0416] 此外根据本发明另一个实施例的配置，将至少一部分内容代码设置为加密数据，在具有分层结构的密钥树中，作为加密密钥应用包含与作为对应于信息处理设备的最底层节点的叶片相对应地设置的装置特有密钥、与从叶片到顶层节点的路径上的节点相对应地设置的组密钥、与顶层节点相对应地设置的装置制造实体 密钥以及与信息处理设备的型号和版本相对应地设置的型号和版本密钥的加密密钥中的任意一个。因此，可以仅允许特定信息处理设备的组对内容代码执行处理。其结果是，可以实现能够防止应用非法内容代码的处理的配置。

[0417] 本领域技术人员应当理解，可以在所附权利要求或其等同物的范围内，根据设计需要和其它因素进行各种变形、组合、子组合和替换。

[0418] 本发明包含2006年2月6日在日本专利局提交的日本特愿JP 2006-028338所涉及的主题，其全部内容通过引用包含与此。

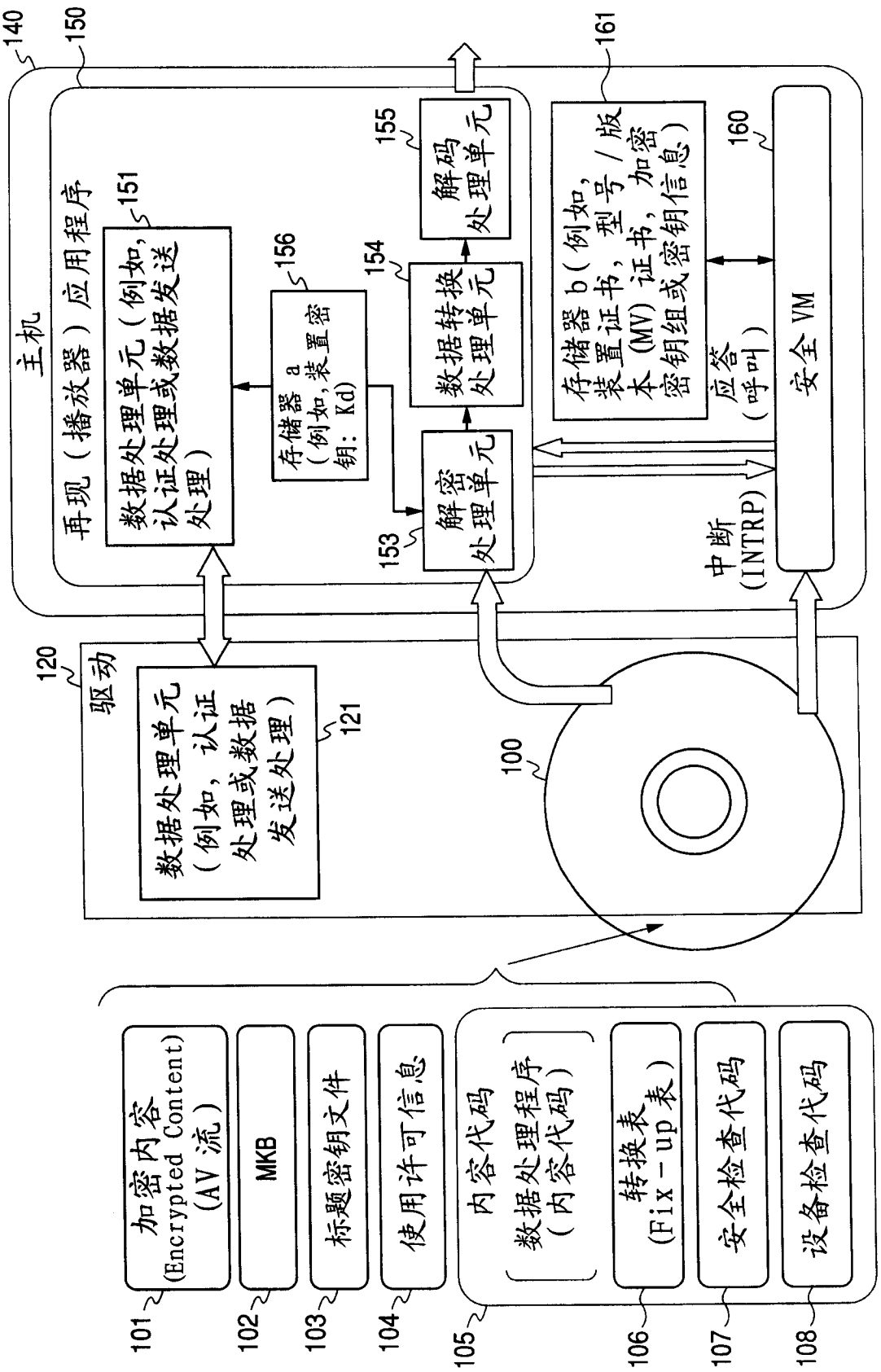

140
150
主机
再现（播放器）应用程序
151
数据处理单元（例如，认证处理或数据发送处理）
156
存储器 a（例如，装置密钥：Kd）
154
数据转换处理单元
155
解码处理单元
153
解密单元
161
存储器 b（例如，装置证书，型号/版本（MV）证书，加密密钥组或密钥信息）
160
安全 VM
应答（呼叫）
中断（INTRP）
120
驱动
数据处理单元（例如，认证处理或数据发送处理）
121
100
101
加密内容（Encrypted Content）（AV 流）
102
MKB
103
标题密钥文件
104
使用许可信息
105
内容代码
数据处理程序（内容代码）
106
转换表（Fix-up 表）
107
安全检查代码
108
设备检查代码

图 1

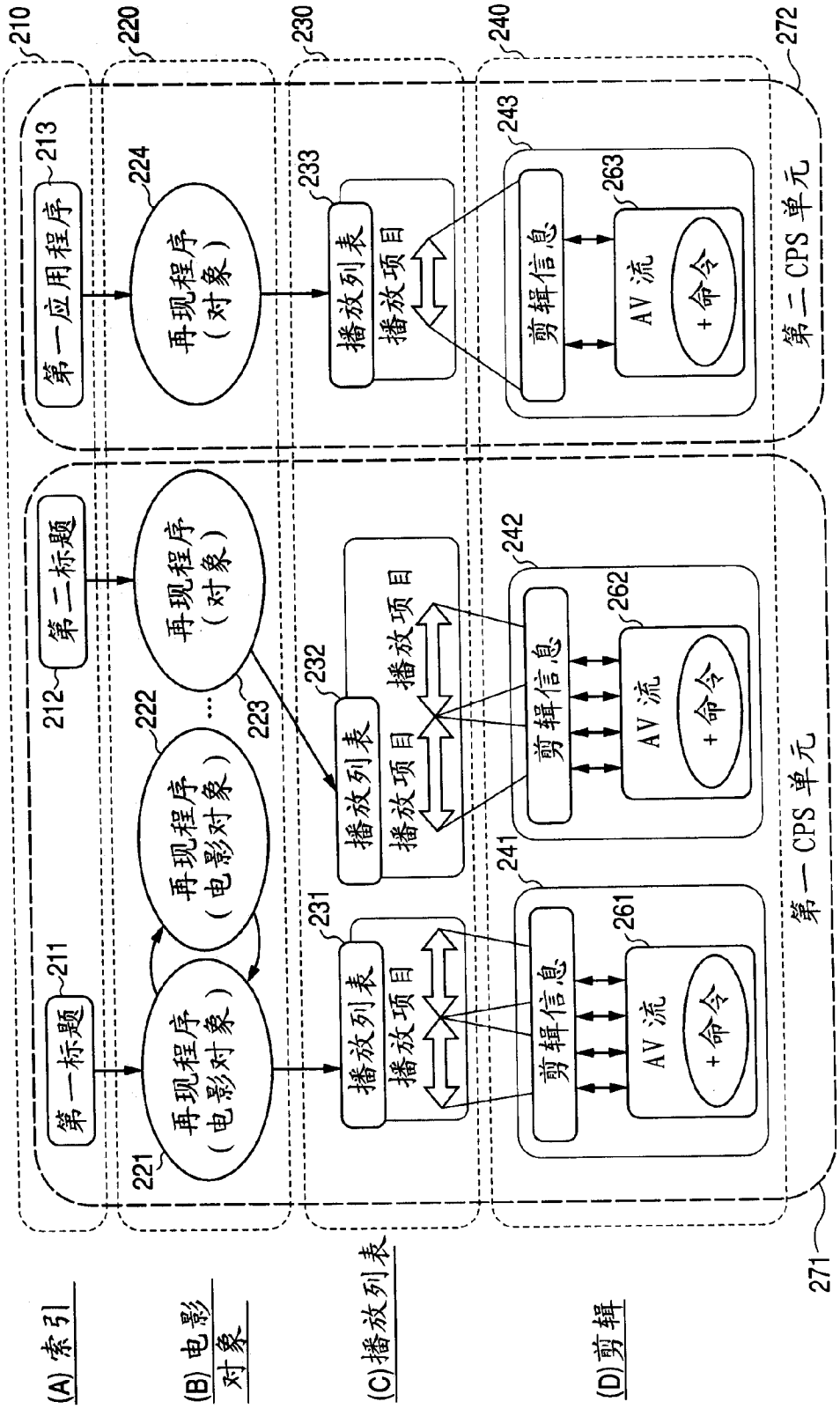

(A) 索引
(B) 电影对象
(C)播放列表
(D)剪辑
210
220
230
240
272
271
第一应用程序
213
224
233
243
263
第二标题
212
222
223
232
242
262
第一标题
211
221
231
241
261
再现程序（对象）
播放列表
播放项目
剪辑信息
AV 流
+命令
第二 CPS 单元
第一 CPS 单元

图 2

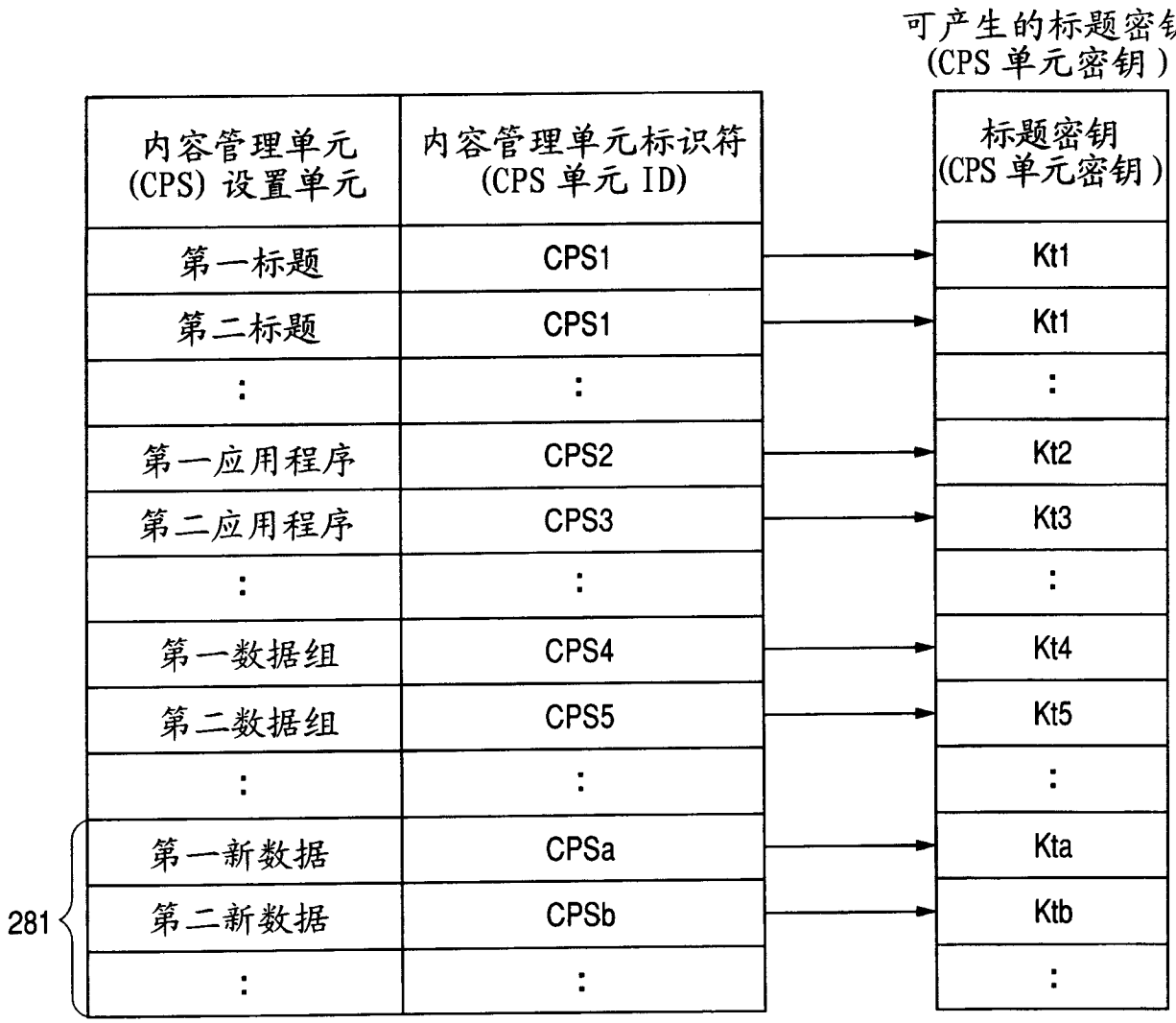

可产生的标题密钥
(CPS 单元密钥)
内容管理单元
(CPS) 设置单元
内容管理单元标识符
(CPS 单元 ID)
标题密钥
(CPS 单元密钥)
第一标题
CPS1
Kt1
第二标题
CPS1
Kt1
:
:
:
第一应用程序
CPS2
Kt2
第二应用程序
CPS3
Kt3
:
:
:
第一数据组
CPS4
Kt4
第二数据组
CPS5
Kt5
:
:
:
281
第一新数据
CPSa
Kta
第二新数据
CPSb
Ktb
:
:
:

图 3

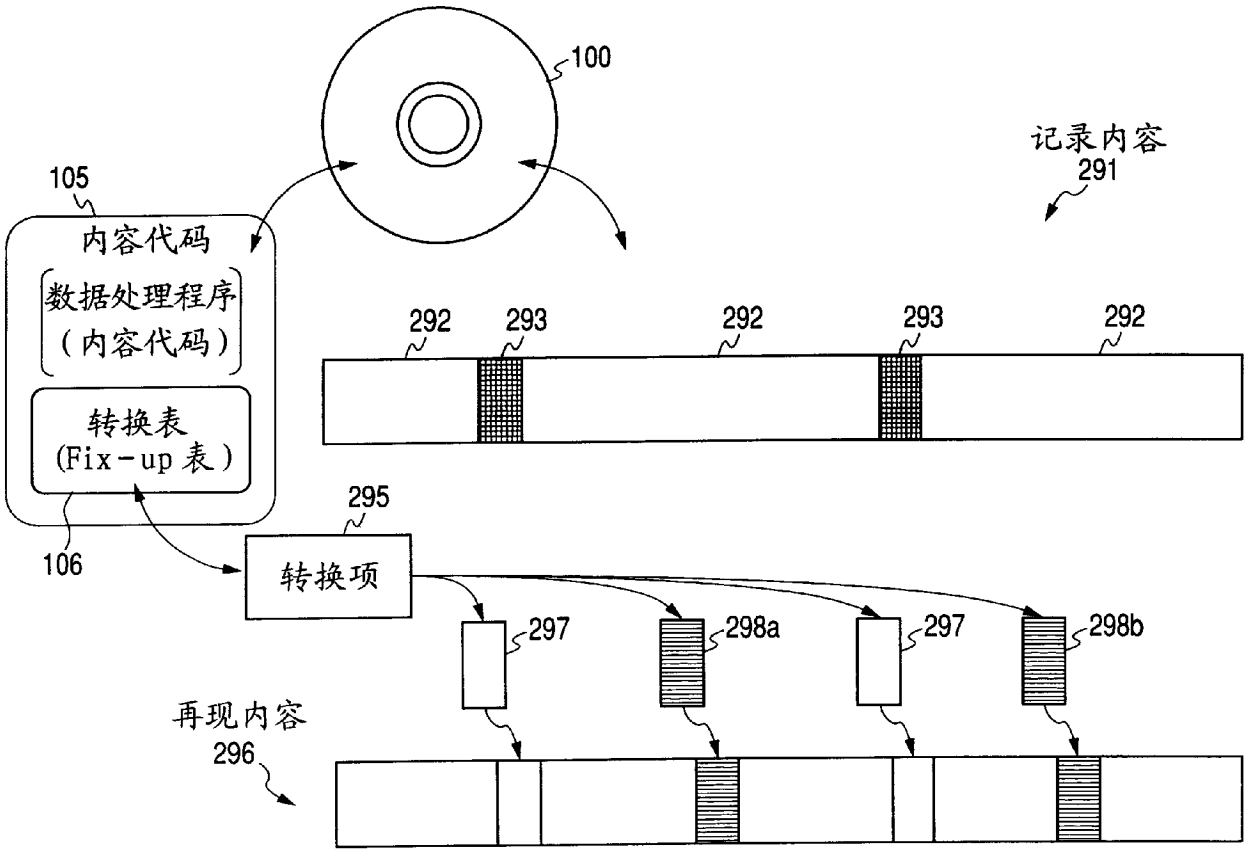

100
记录内容
291
105
内容代码
数据处理程序
(内容代码)
转换表
(Fix-up 表)
106
292
293
292
293
292
295
转换项
297
298a
297
298b
再现内容
296

图 4

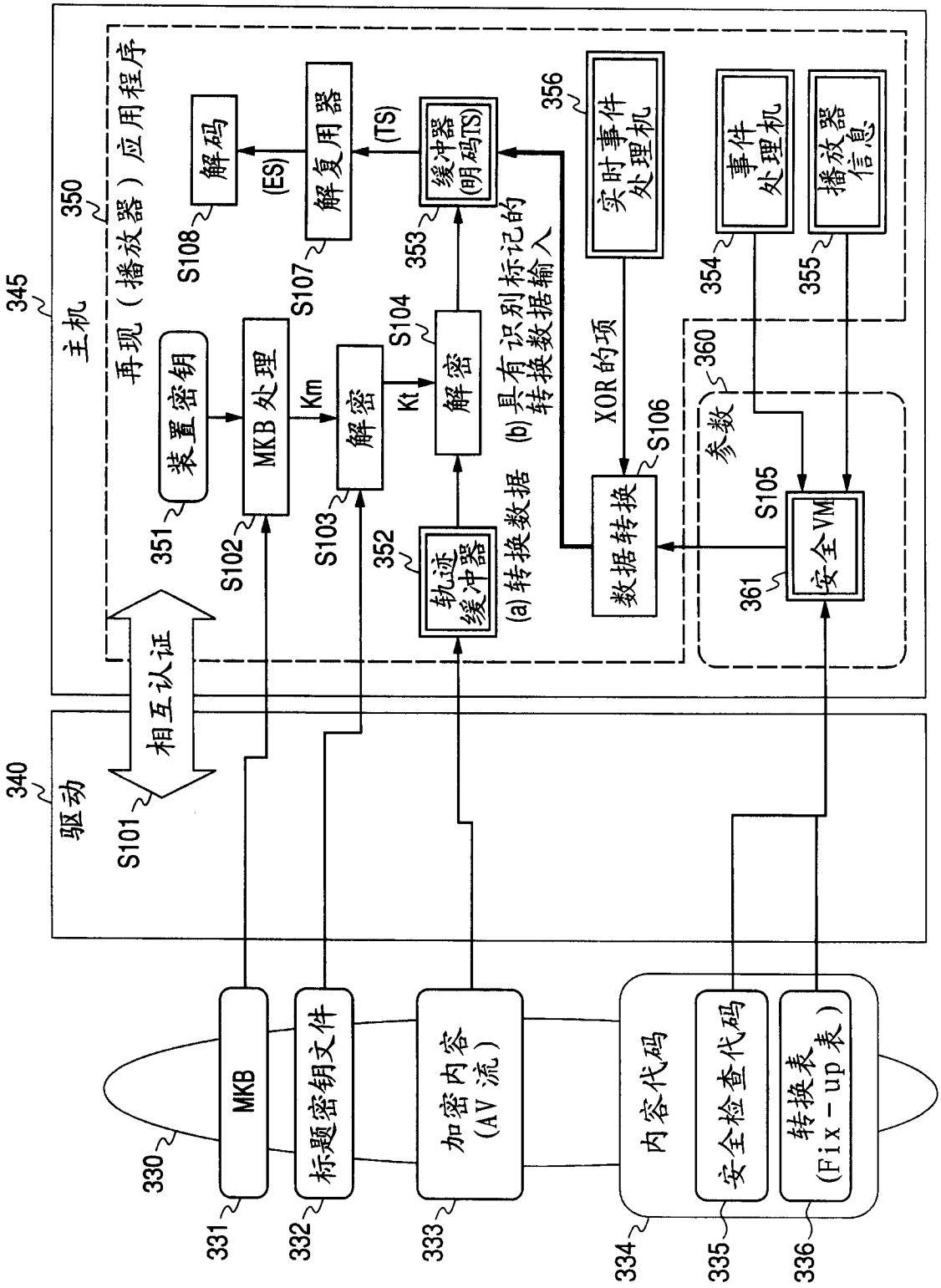

345
主机
350
再现（播放器）应用程序
340
驱动
S101
相互认证
351
装置密钥
S102
MKB 处理
Km
S103
解密
Kt
S104
解密
352
轨迹缓冲器
(a) 转换数据
(b) 具有识别标记的转换数据输入
S107
解复用器
(TS)
S108
解码
(ES)
353
缓冲器(明码TS)
356
实时事件处理机
XOR 的项
S106
数据转换
361
安全 VM
S105
360
参数
354
事件处理机
355
播放器信息
330
331
MKB
332
标题密钥文件
333
加密内容(AV 流)
334
内容代码
335
安全检查代码
336
转换表(Fix-up 表)

图 5

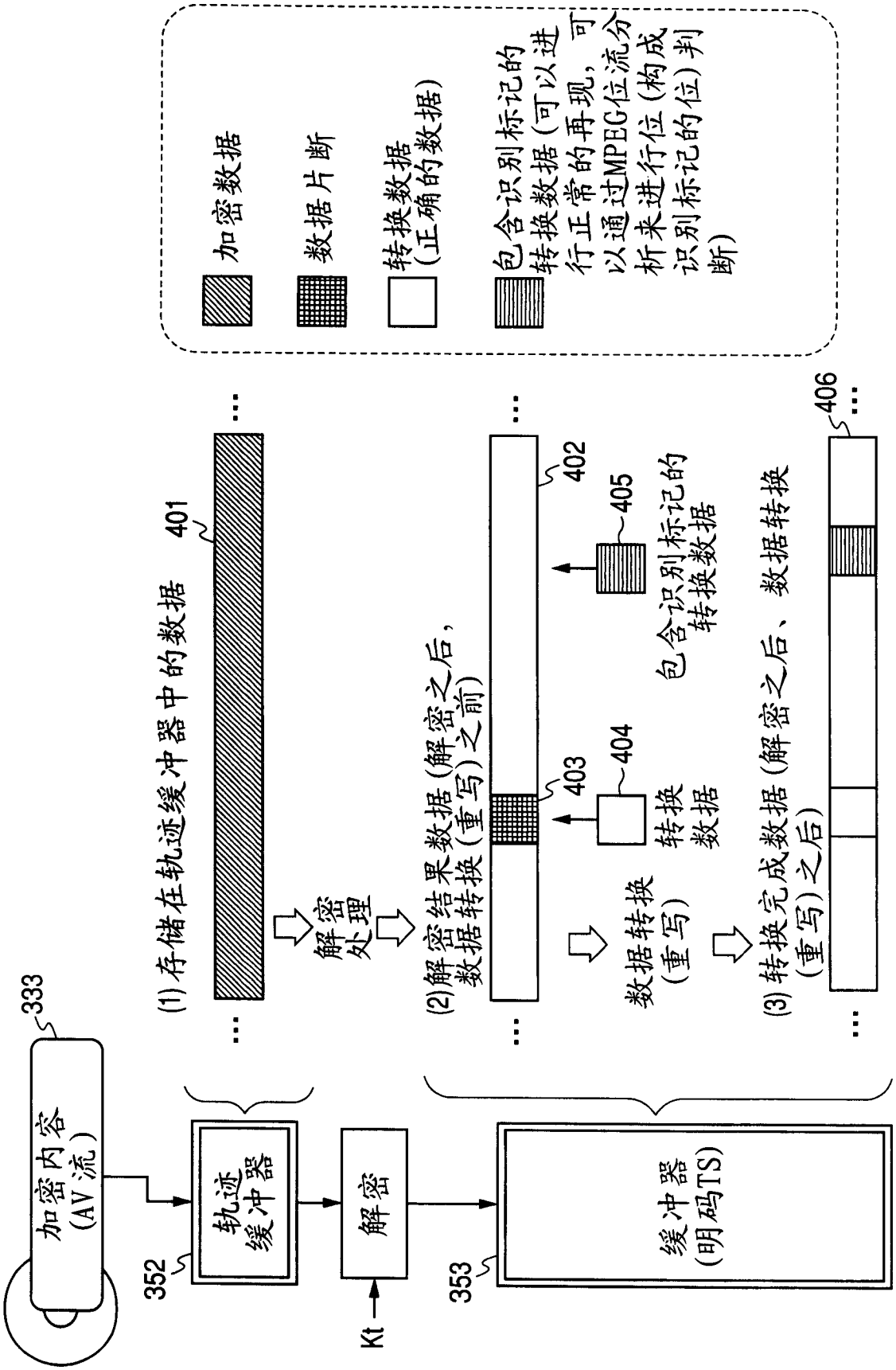

加密数据
数据片断
转换数据
(正确的数据)
包含识别标记的
转换数据(可以进
行正常的再现，可
以通过MPEG位流分
析来进行位(构成
识别标记的位)判
断)
加密内容
(AV流)
333
352
轨迹
缓冲器
解密
Kt
353
缓冲器
(明码TS)
(1)存储在轨迹缓冲器中的数据
401
解密
处理
(2)解密结果数据(解密之后，
数据转换(重写)之前)
402
403
404
405
数据转换
(重写)
转换
数据
包含识别标记的
转换数据
(3)转换完成数据(解密之后、数据转换
(重写)之后)
406

图 6

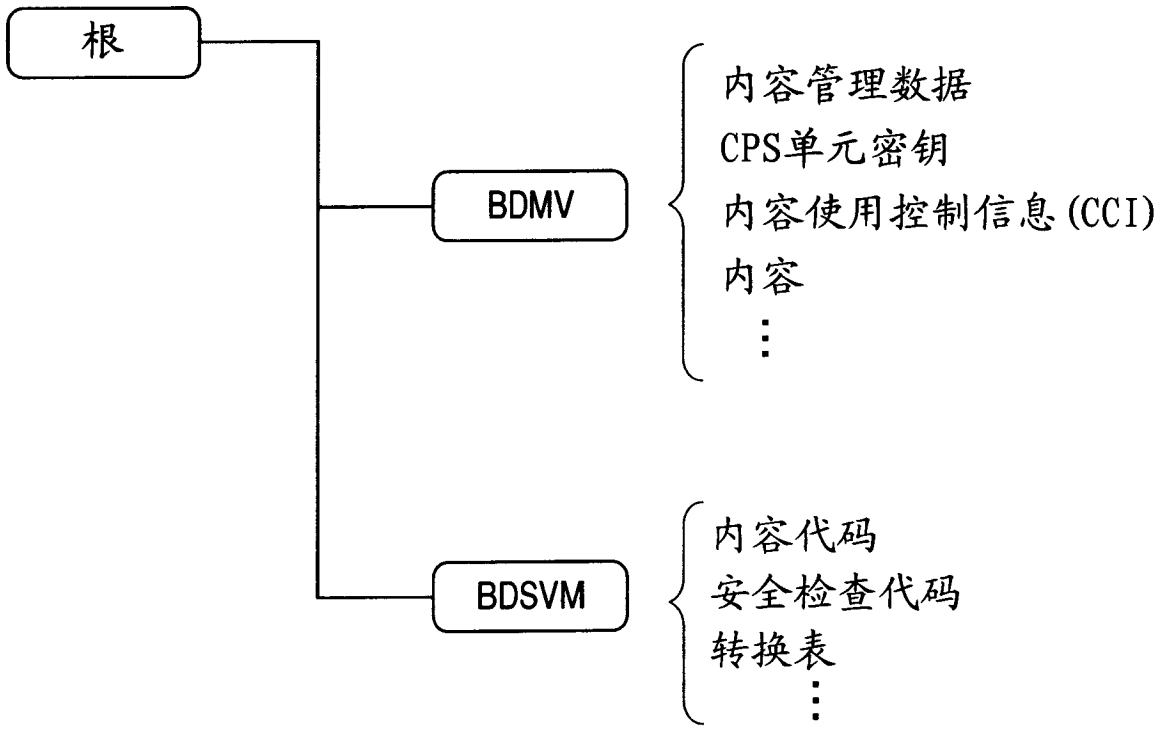


图 7

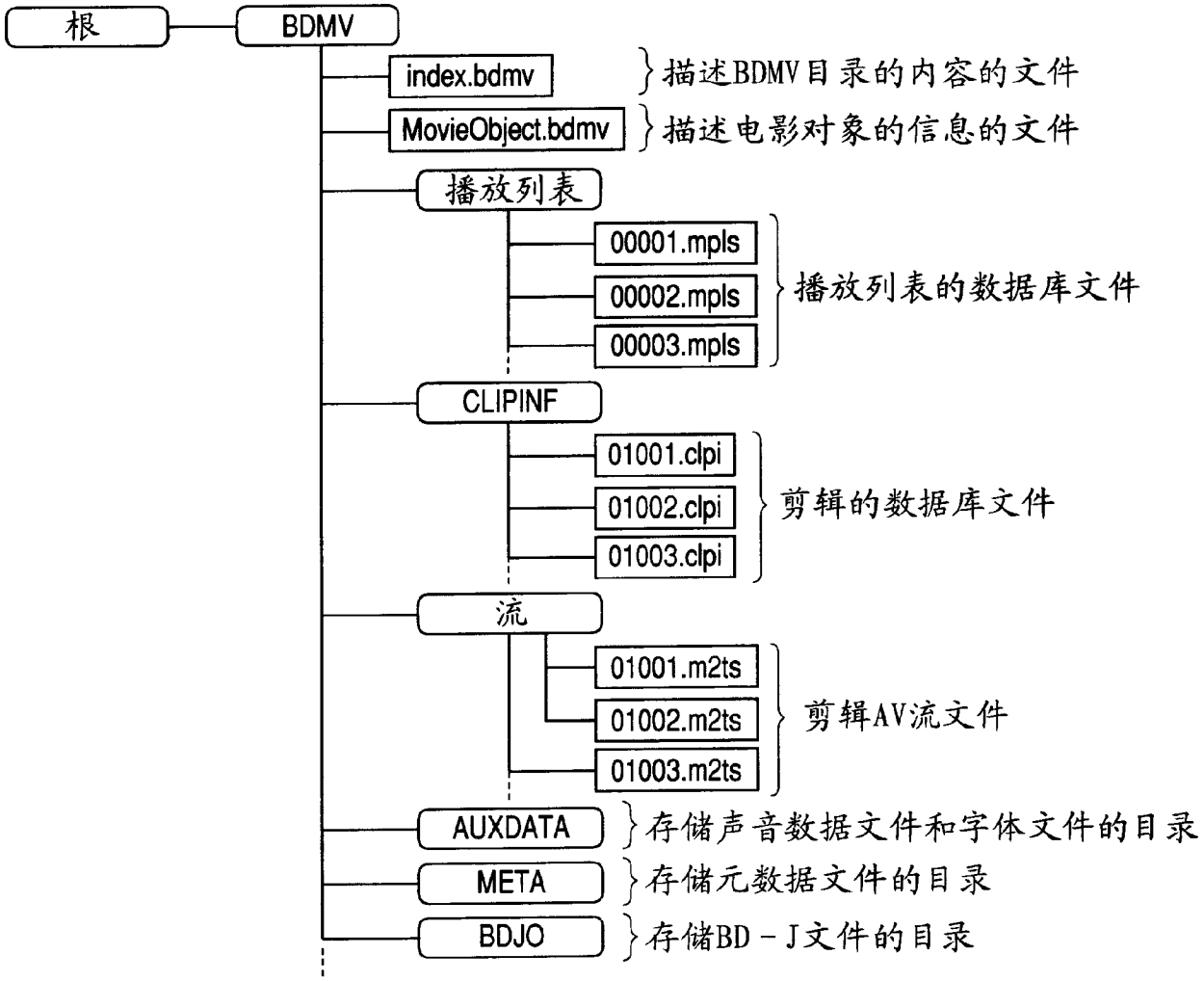

根
BDMV
index.bdmv
描述BDMV目录的内容的文件
MovieObject.bdmv
描述电影对象的信息的文件
播放列表
00001.mpls
00002.mpls
00003.mpls
播放列表的数据库文件
CLIPINF
01001.clpi
01002.clpi
01003.clpi
剪辑的数据库文件
流
01001.m2ts
01002.m2ts
01003.m2ts
剪辑AV流文件
AUXDATA
存储声音数据文件和字体文件的目录
META
存储元数据文件的目录
BDJO
存储BD－J文件的目录

图 8

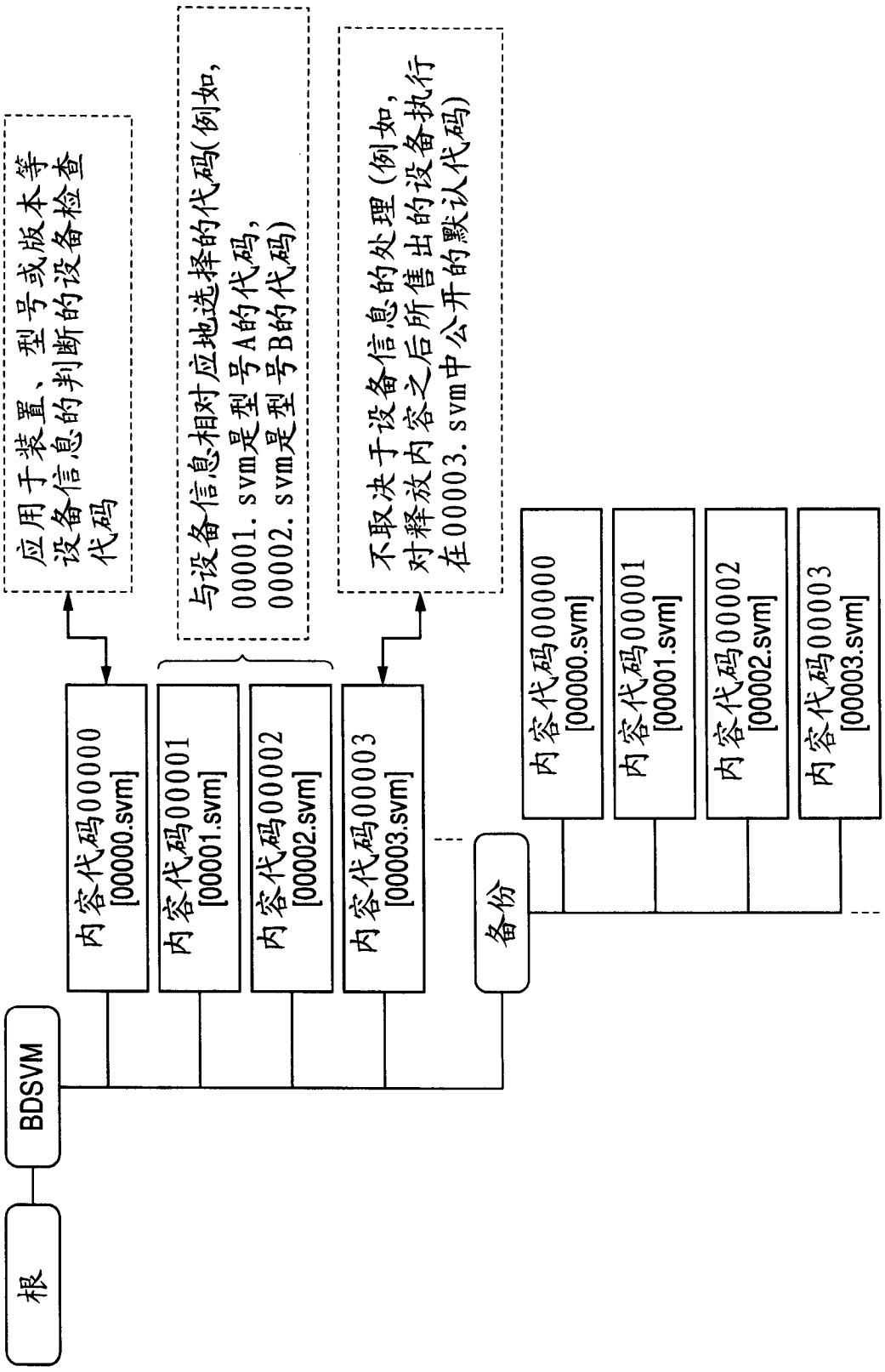

根
BDSVM
内容代码00000 [00000.svm]
内容代码00001 [00001.svm]
内容代码00002 [00002.svm]
内容代码00003 [00003.svm]
备份
内容代码00000 [00000.svm]
内容代码00001 [00001.svm]
内容代码00002 [00002.svm]
内容代码00003 [00003.svm]
应用于装置、型号或版本等设备信息的判断的设备检查代码
与设备信息相对应地选择的代码(例如，00001.svm是型号A的代码，00002.svm是型号B的代码)
不取决于设备信息的处理(例如，对释放内容之后所售出的设备执行在00003.svm中公开的默认代码)

图 9

装置证书 (Device CERT (4 × 41 = 164字节))
装置证书大小 (DeviceCertificateSize)
装置证书版本 (DeviceCertificateVersion)
装置制造商标识符 (DeviceManufacturerID)
装置标识符 (DeviceID)
保留 (reserved)
装置证书签名日期 (DeviceCertificateSigningDate)
装置公共密钥 (DevicePublicKey)
装置证书签名 (DeviceCertificateSignature (by KIC))

图 10A

型号/版本证书 (Model/Version CERT (4 × 41 = 172字节))
型号/版本证书大小 (ModelCertificateSize)
型号/版本证书版本 (ModelCertificateVersion)
型号制造商标识符 (ModelManufacturerID)
型号标识符 (Model ID)
版本标识符 (Version ID)
修正标识符 (RevisionID)
保留 (reserved)
型号/版本证书签名日期 (ModelCertificateSigningDate)
型号/版本公共密钥 (Model/Version PublicKey)
mw@. 版本证书签名 (ModelCertificateSignature (by KIC))

图 10B

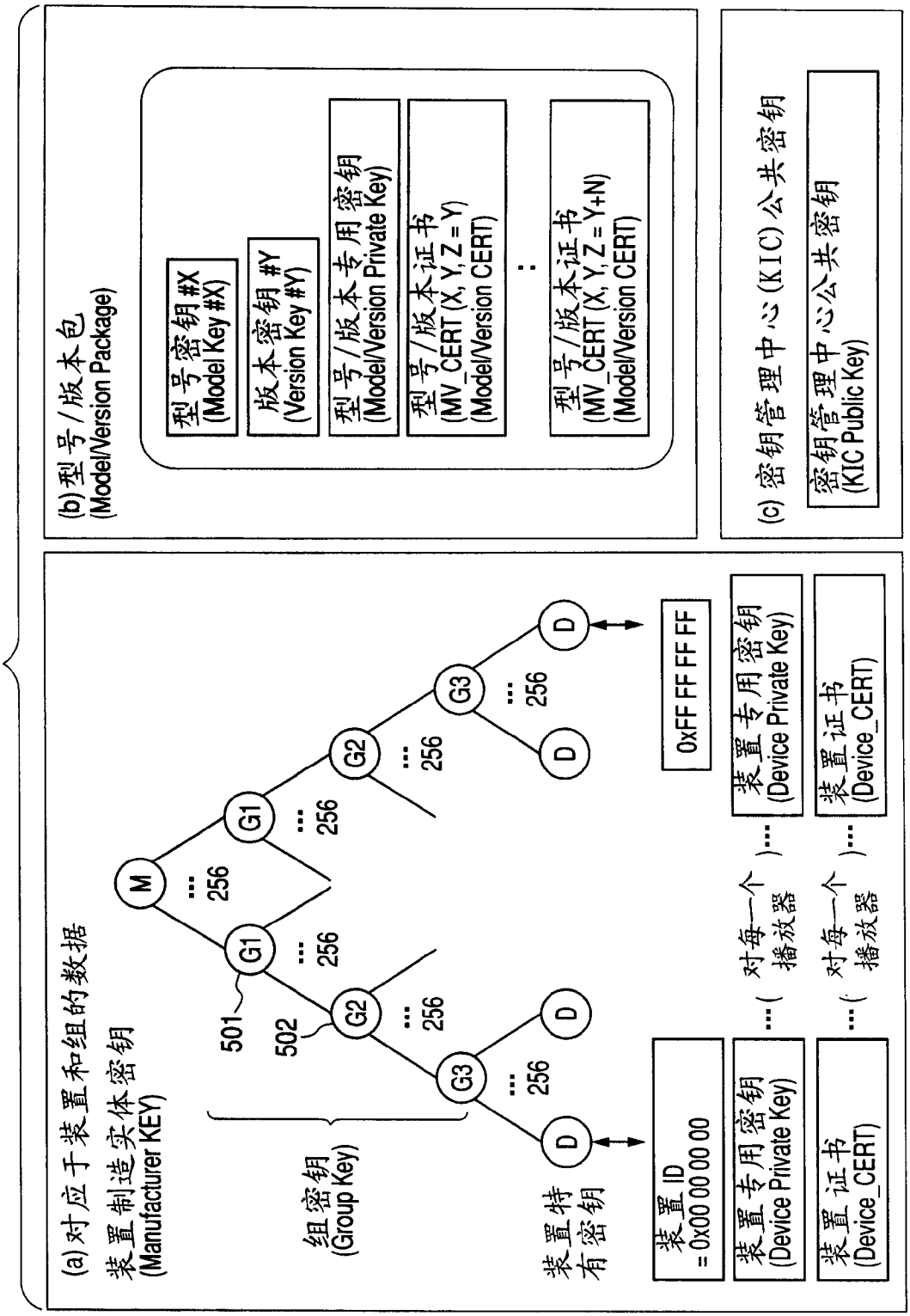

(a) 对应于装置和组的数据
装置制造实体密钥
(Manufacturer KEY)
M
G1
G2
G3
D
...
256
501
502
组密钥
(Group Key)
装置特有密钥
装置 ID
= 0x00 00 00 00
0xFF FF FF FF
装置专用密钥
(Device Private Key)
装置证书
(Device_CERT)
...(对每一个播放器)...
(b) 型号/版本包
(Model/Version Package)
型号密钥 #X
(Model Key #X)
版本密钥 #Y
(Version Key #Y)
型号/版本专用密钥
(Model/Version Private Key)
型号/版本证书
(MV_CERT (X, Y, Z = Y)
(Model/Version CERT)
型号/版本证书
(MV_CERT (X, Y, Z = Y+N)
(Model/Version CERT)
(c) 密钥管理中心 (KIC) 公共密钥
密钥管理中心公共密钥
(KIC Public Key)

图 11

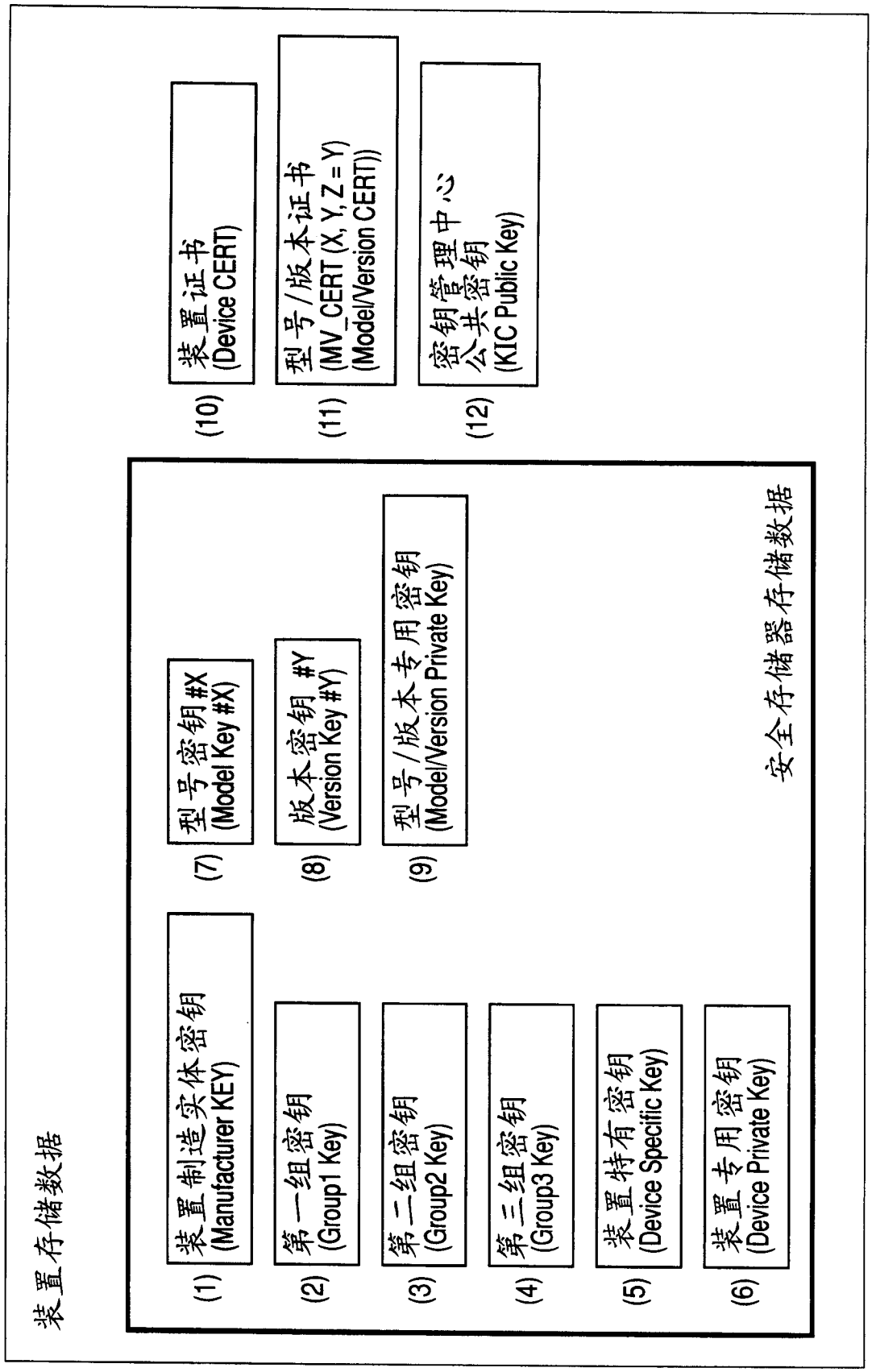

装置存储数据
(1) 装置制造实体密钥 (Manufacturer KEY)
(2) 第一组密钥 (Group1 Key)
(3) 第二组密钥 (Group2 Key)
(4) 第三组密钥 (Group3 Key)
(5) 装置特有密钥 (Device Specific Key)
(6) 装置专用密钥 (Device Private Key)
(7) 型号密钥 #X (Model Key #X)
(8) 版本密钥 #Y (Version Key #Y)
(9) 型号/版本专用密钥 (Model/Version Private Key)
安全存储器存储数据
(10) 装置证书 (Device CERT)
(11) 型号/版本证书 (MV_CERT (X, Y, Z = Y) (Model/Version CERT))
(12) 密钥管理中心公共密钥 (KIC Public Key)

图 12

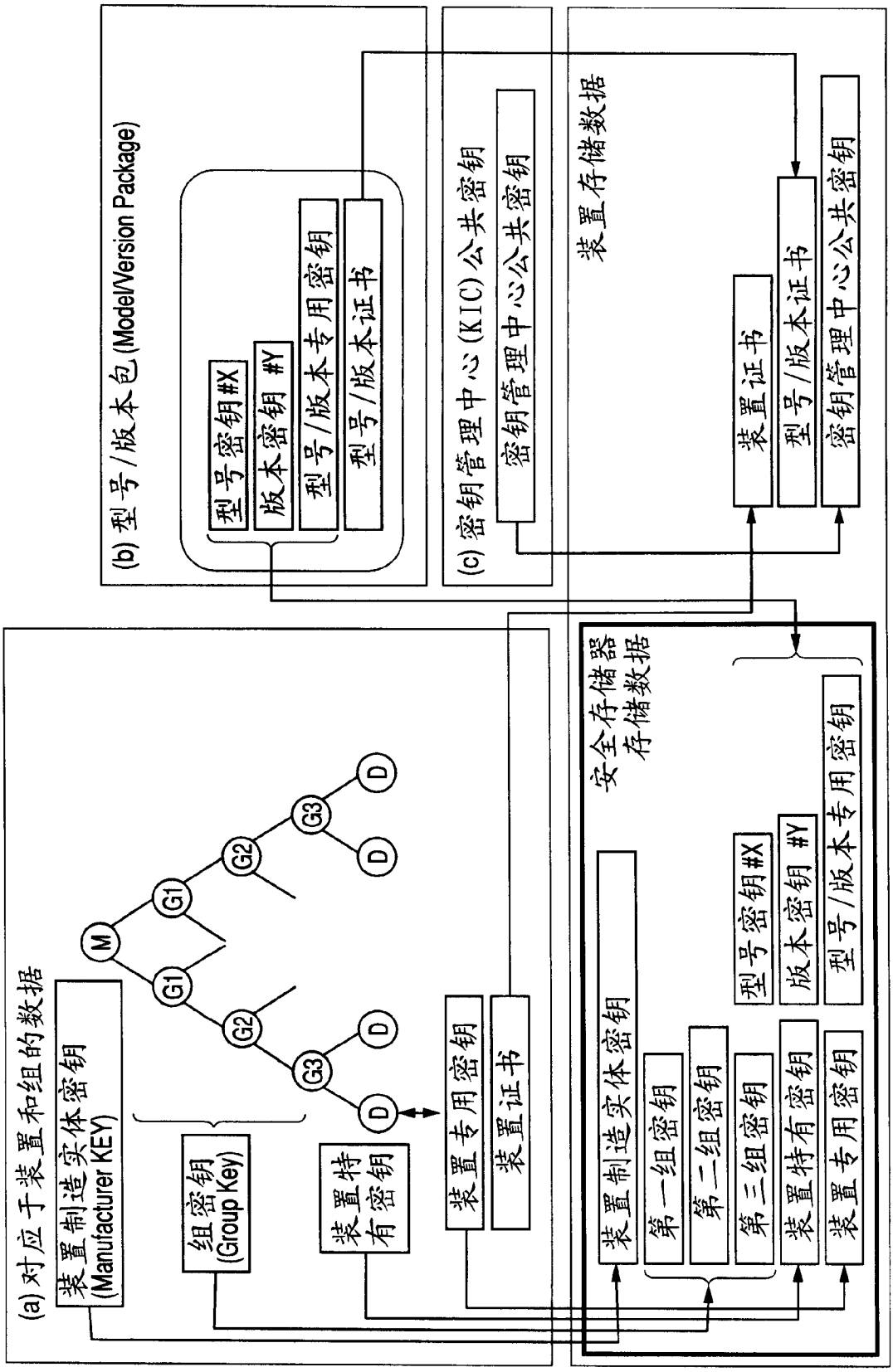

(a) 对应于装置和组的数据
装置制造实体密钥 (Manufacturer KEY)
组密钥 (Group Key)
装置特有密钥
装置专用密钥
装置证书
M
G1
G2
G3
D
(b) 型号/版本包 (Model/Version Package)
型号密钥#X
版本密钥 #Y
型号/版本专用密钥
型号/版本证书
(c) 密钥管理中心 (KIC) 公共密钥
密钥管理中心公共密钥
装置存储数据
安全存储器存储数据
装置制造实体密钥
第一组密钥
第二组密钥
第三组密钥
装置特有密钥
装置专用密钥
型号密钥#X
版本密钥 #Y
型号/版本专用密钥
装置证书
型号/版本证书
密钥管理中心公共密钥

图 13

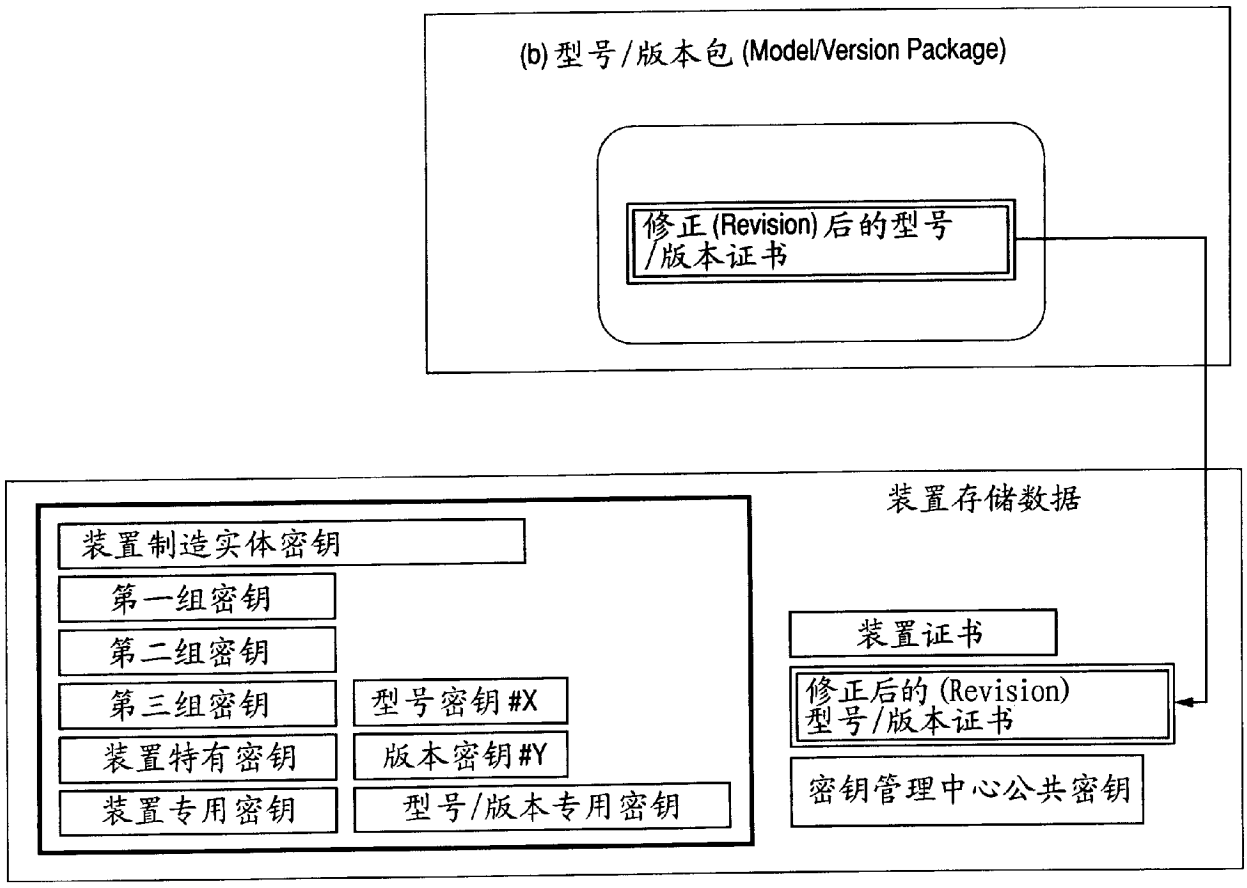

(b) 型号/版本包 (Model/Version Package)
修正 (Revision) 后的型号/版本证书
装置存储数据
装置制造实体密钥
第一组密钥
第二组密钥
第三组密钥
装置特有密钥
装置专用密钥
型号密钥 #X
版本密钥 #Y
型号/版本专用密钥
装置证书
修正后的 (Revision) 型号/版本证书
密钥管理中心公共密钥

图 14

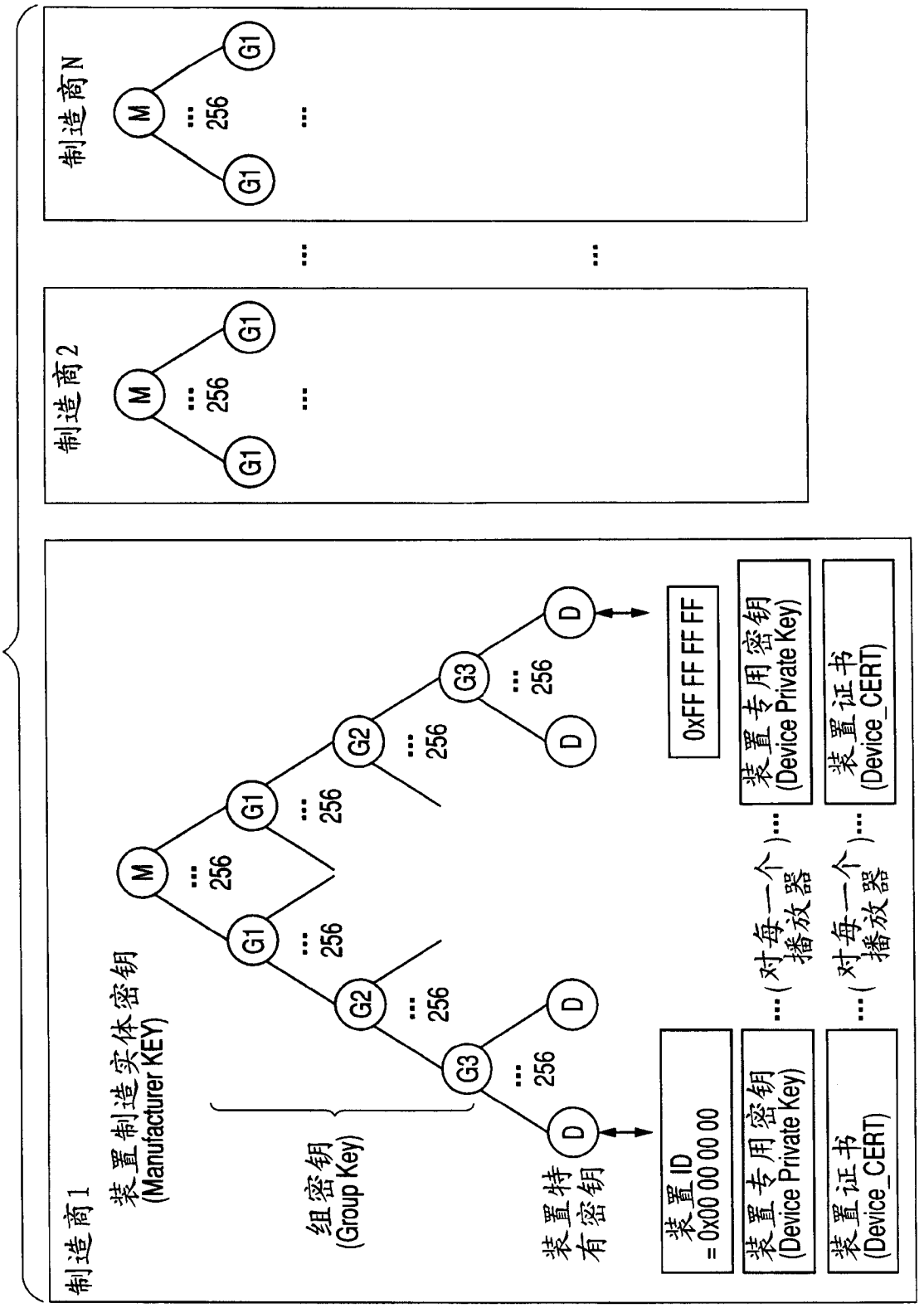

制造商1
装置制造实体密钥
(Manufacturer KEY)
M
G1
G2
G3
D
256
组密钥
(Group Key)
装置特有密钥
装置 ID
= 0x00 00 00 00
0xFF FF FF FF
装置专用密钥
(Device Private Key)
装置证书
(Device_CERT)
...(对每一个播放器)...
装置专用密钥
(Device Private Key)
装置证书
(Device_CERT)
制造商2
制造商N

图 15

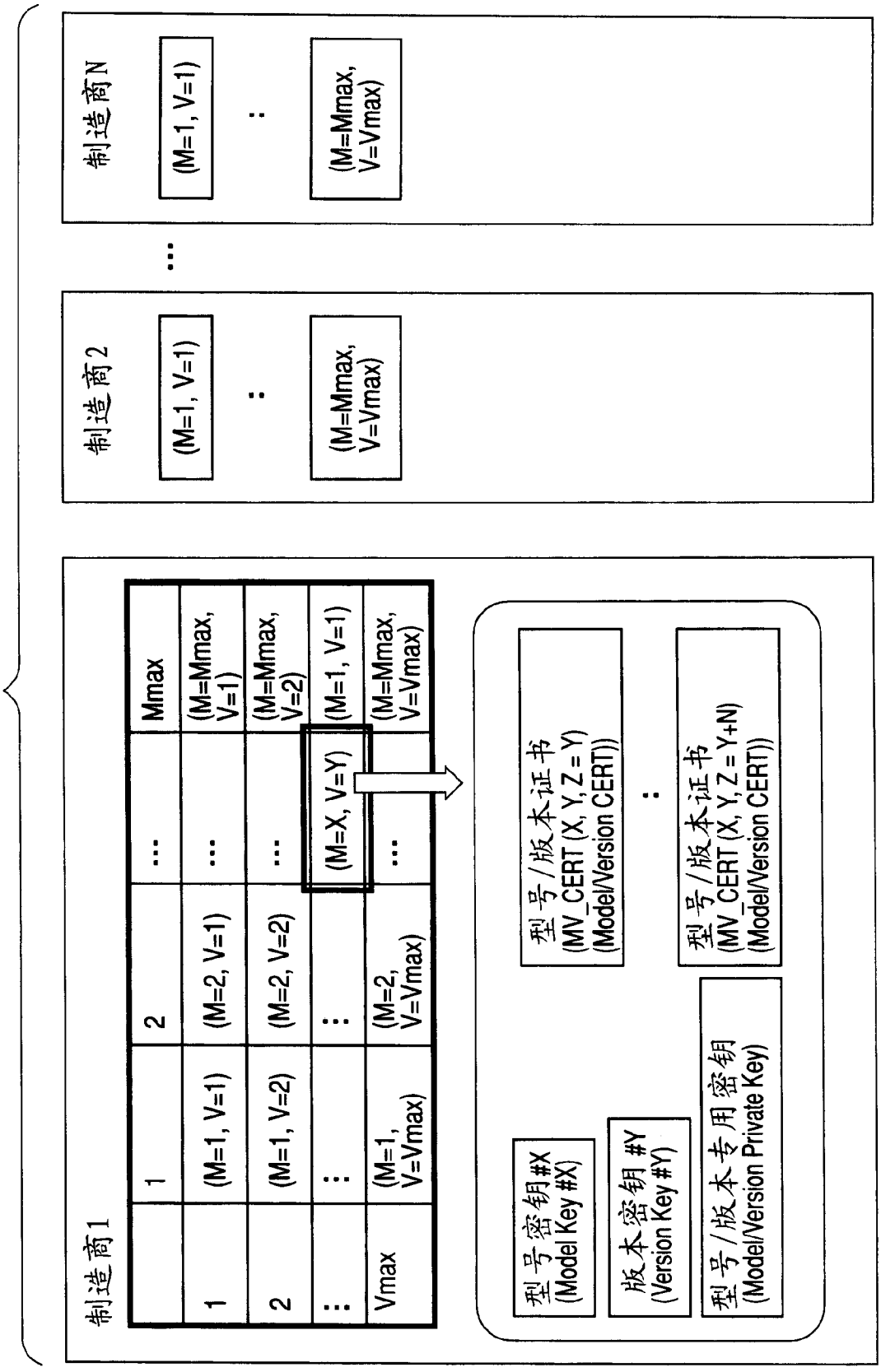

制造商1
制造商2
制造商N
(M=1, V=1)
(M=Mmax, V=Vmax)
1
2
Mmax
Vmax
(M=X, V=Y)
型号密钥#X
(Model Key #X)
版本密钥 #Y
(Version Key #Y)
型号/版本专用密钥
(Model/Version Private Key)
型号/版本证书
(MV_CERT (X, Y, Z = Y)
(Model/Version CERT))
型号/版本证书
(MV_CERT (X, Y, Z = Y+N)
(Model/Version CERT))

图 16

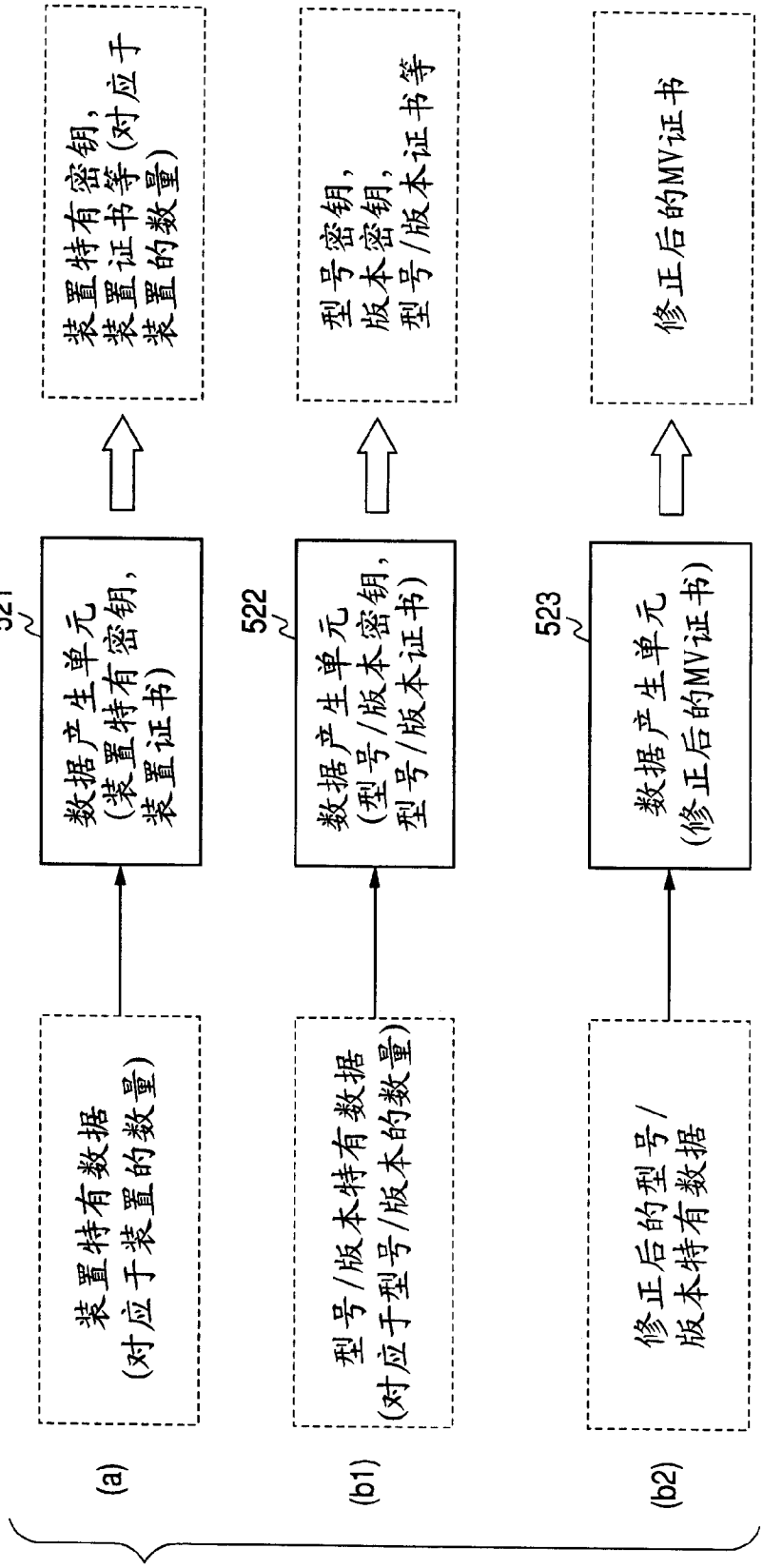

装置特有数据
(对应于装置的数量)
(a)
521
数据产生单元
(装置特有密钥,
装置证书)
装置特有密钥,
装置证书等(对应于
装置的数量)
型号/版本特有数据
(对应于型号/版本的数量)
(b1)
522
数据产生单元
(型号/版本密钥,
型号/版本证书)
型号密钥,
版本密钥,
型号/版本证书等
修正后的型号/
版本特有数据
(b2)
523
数据产生单元
(修正后的MV证书)
修正后的MV证书

图 17

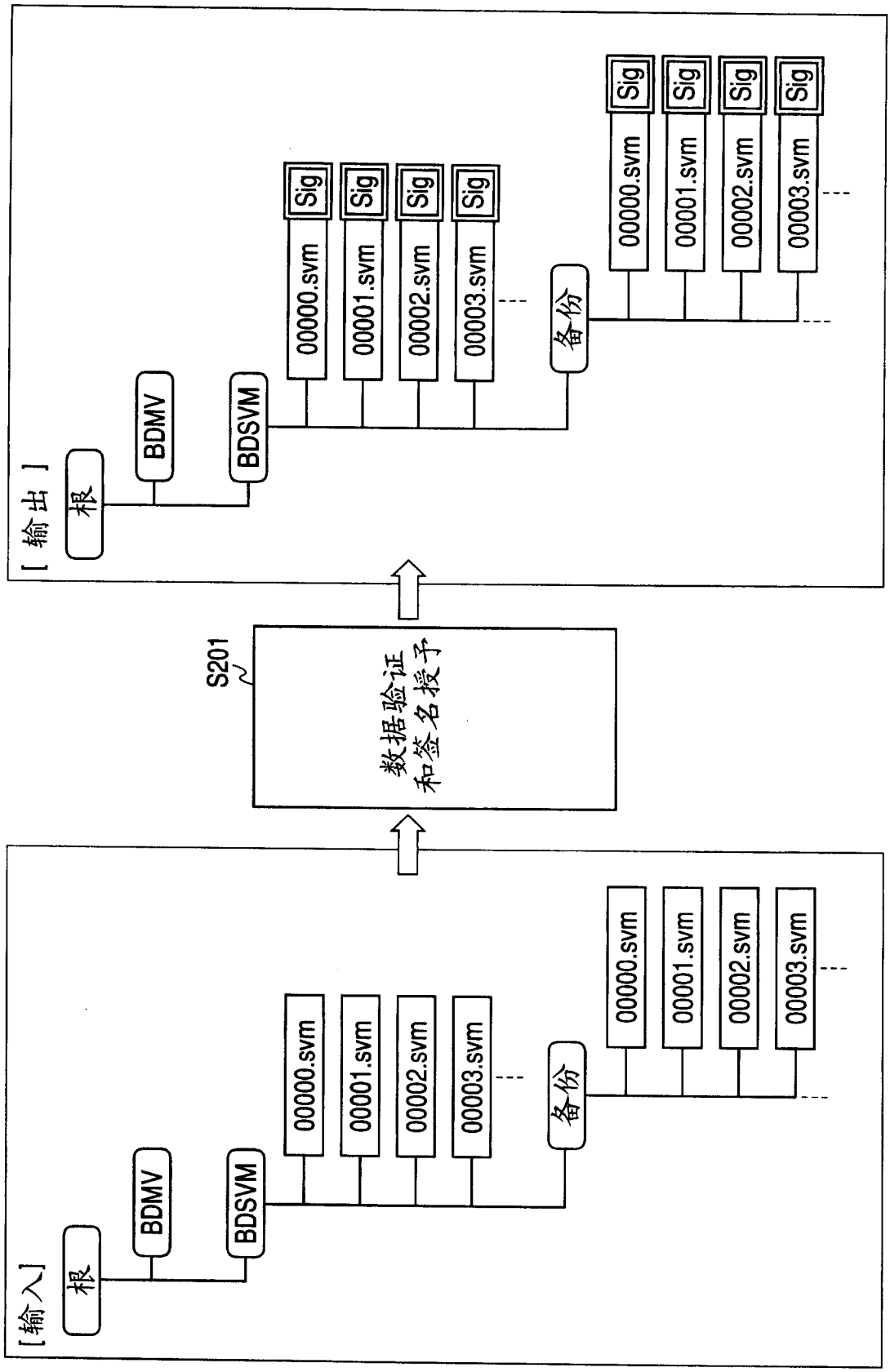

[输入]
根
BDMV
BDSVM
00000.svm
00001.svm
00002.svm
00003.svm
备份
00000.svm
00001.svm
00002.svm
00003.svm
S201
数据验证和签名授予
[输出]
根
BDMV
BDSVM
Sig
00000.svm
Sig
00001.svm
Sig
00002.svm
Sig
00003.svm
备份
Sig
00000.svm
Sig
00001.svm
Sig
00002.svm
Sig
00003.svm

图 18

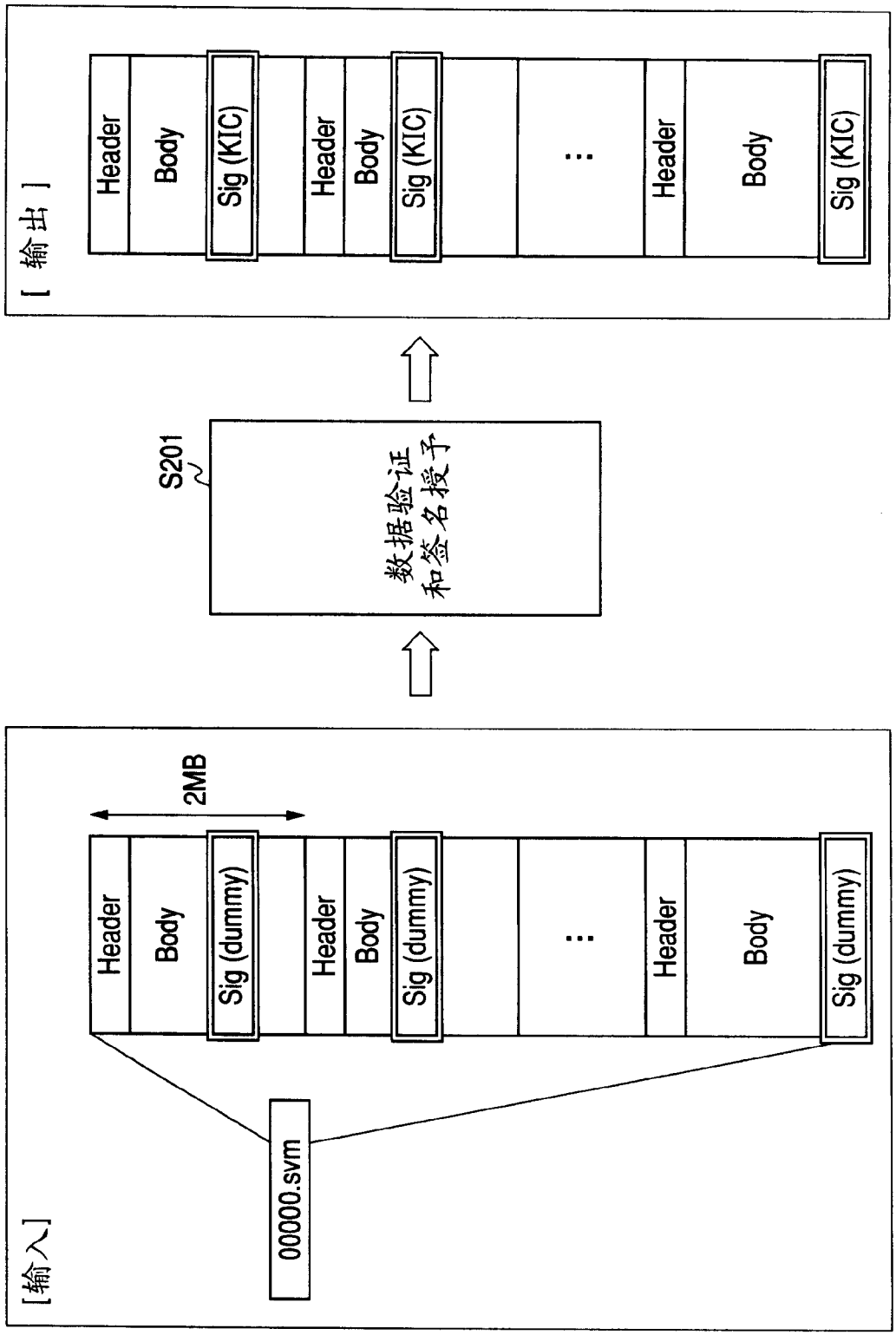

[输入]
00000.svm
2MB
Header
Body
Sig (dummy)
Header
Body
Sig (dummy)
...
Header
Body
Sig (dummy)
S201
数据验证和签名授予
[输出]
Header
Body
Sig (KIC)
Header
Body
Sig (KIC)
...
Header
Body
Sig (KIC)

图 19

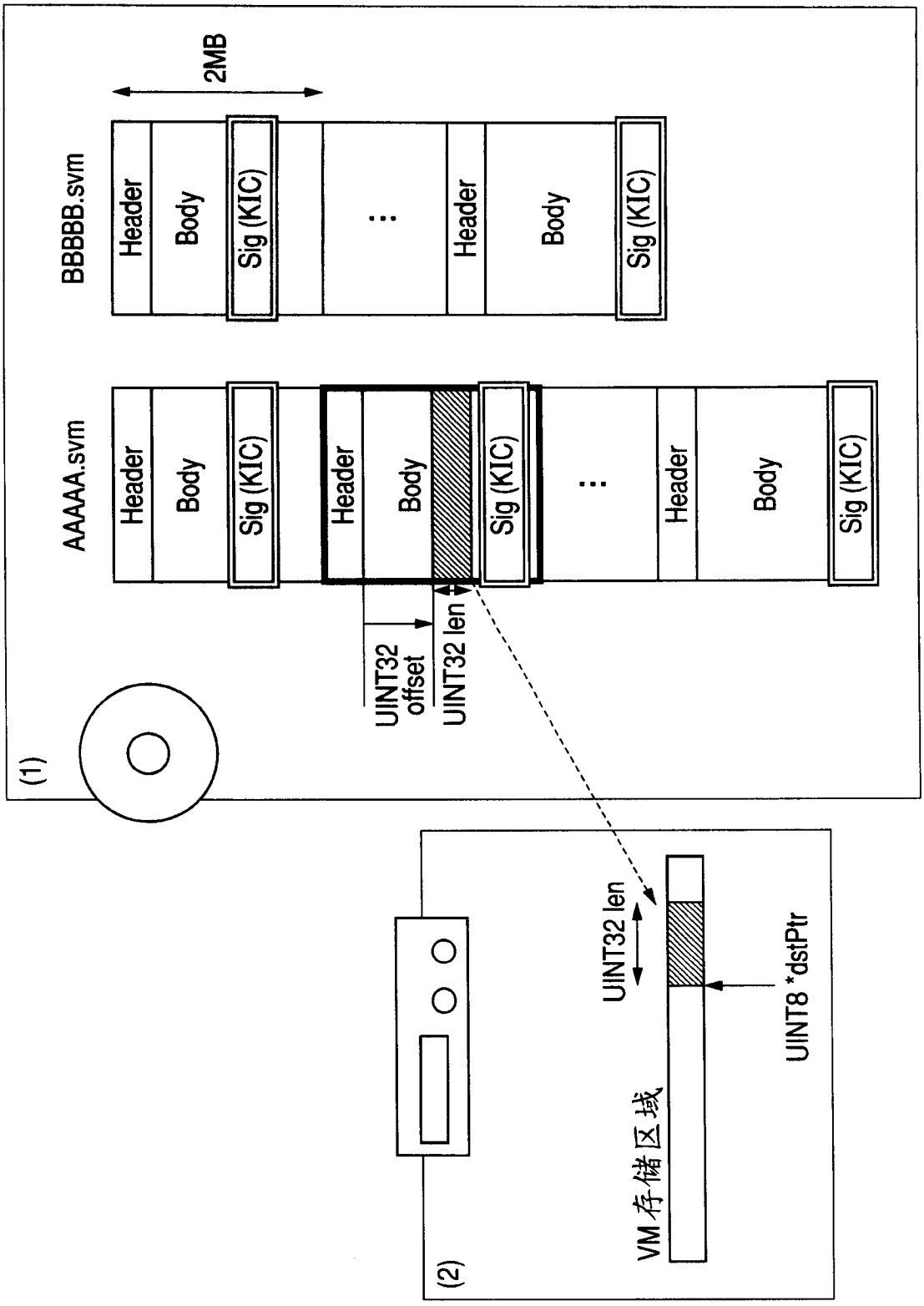

(1)
AAAAA.svm
BBBBB.svm
2MB
Header
Body
Sig (KIC)
UINT32 offset
UINT32 len
(2)
VM存储区域
UINT32 len
UINT8 *dstPtr

图 20

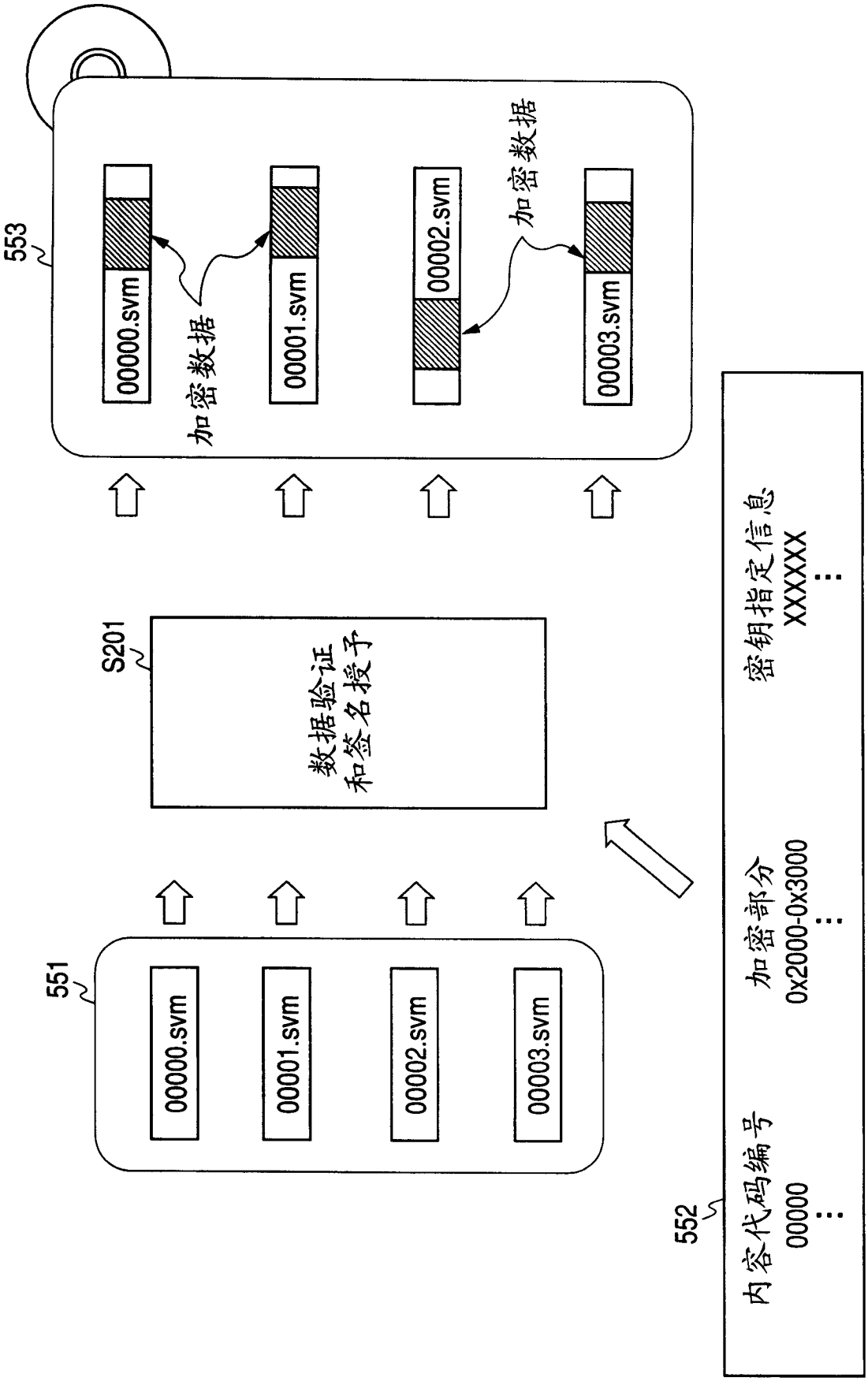

553
00000.svm
加密数据
00001.svm
00002.svm
加密数据
00003.svm
S201
数据验证
和签名授予
551
00000.svm
00001.svm
00002.svm
00003.svm
552
内容代码编号
00000
加密部分
0x2000-0x3000
密钥指定信息
XXXXXX

图 21

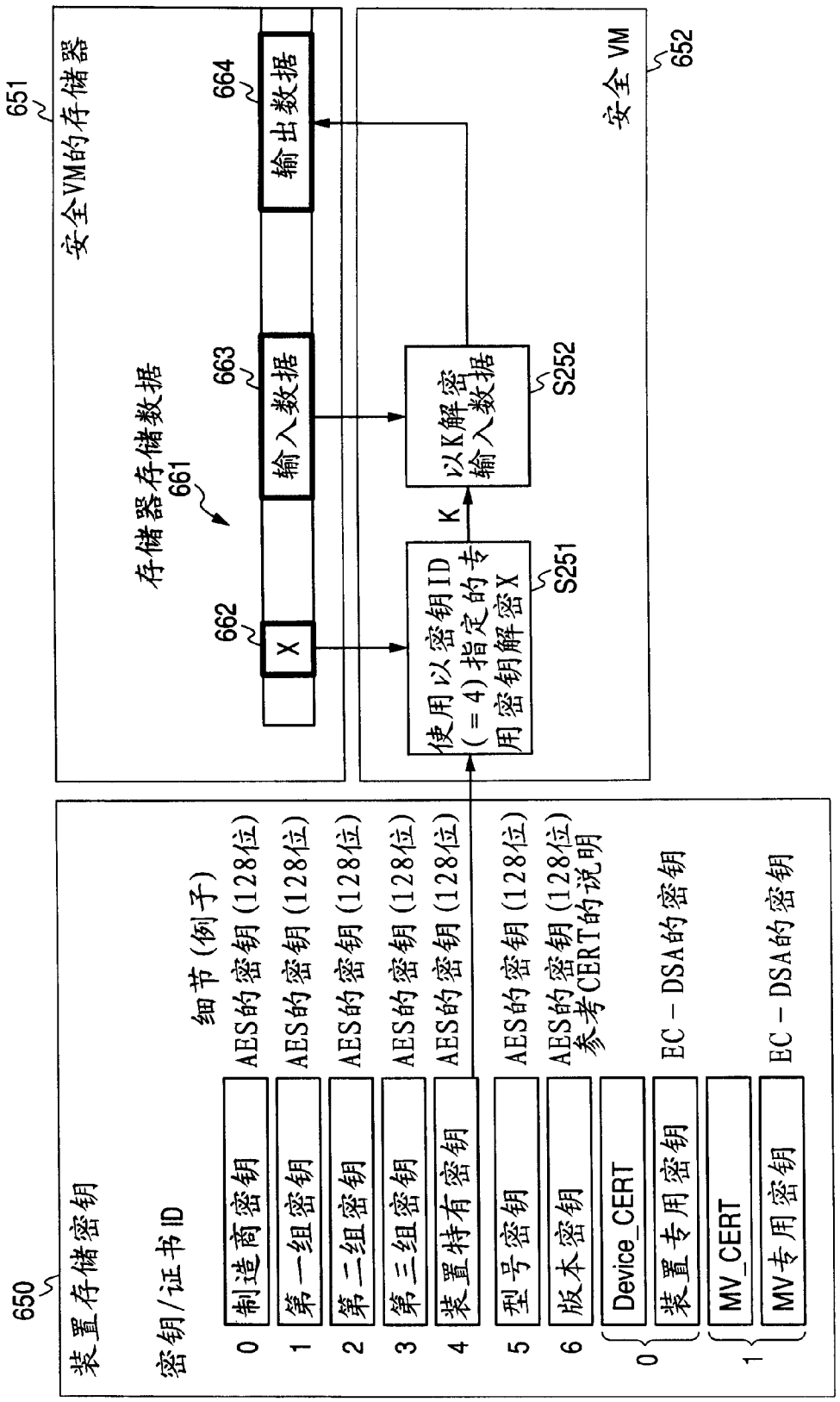

650
装置存储密钥
密钥/证书ID
细节（例子）
0 制造商密钥 AES的密钥（128位）
1 第一组密钥 AES的密钥（128位）
2 第二组密钥 AES的密钥（128位）
3 第三组密钥 AES的密钥（128位）
4 装置特有密钥 AES的密钥（128位）
5 型号密钥 AES的密钥（128位）
6 版本密钥 AES的密钥（128位）
0 Device_CERT 参考CERT的说明
装置专用密钥 EC－DSA的密钥
1 MV_CERT
MV专用密钥 EC－DSA的密钥
651
安全VM的存储器
存储器存储数据
661
662
X
663
输入数据
664
输出数据
使用以密钥ID（＝4）指定的专用密钥解密X
S251
K
以K解密输入数据
S252
安全 VM
652

图 22

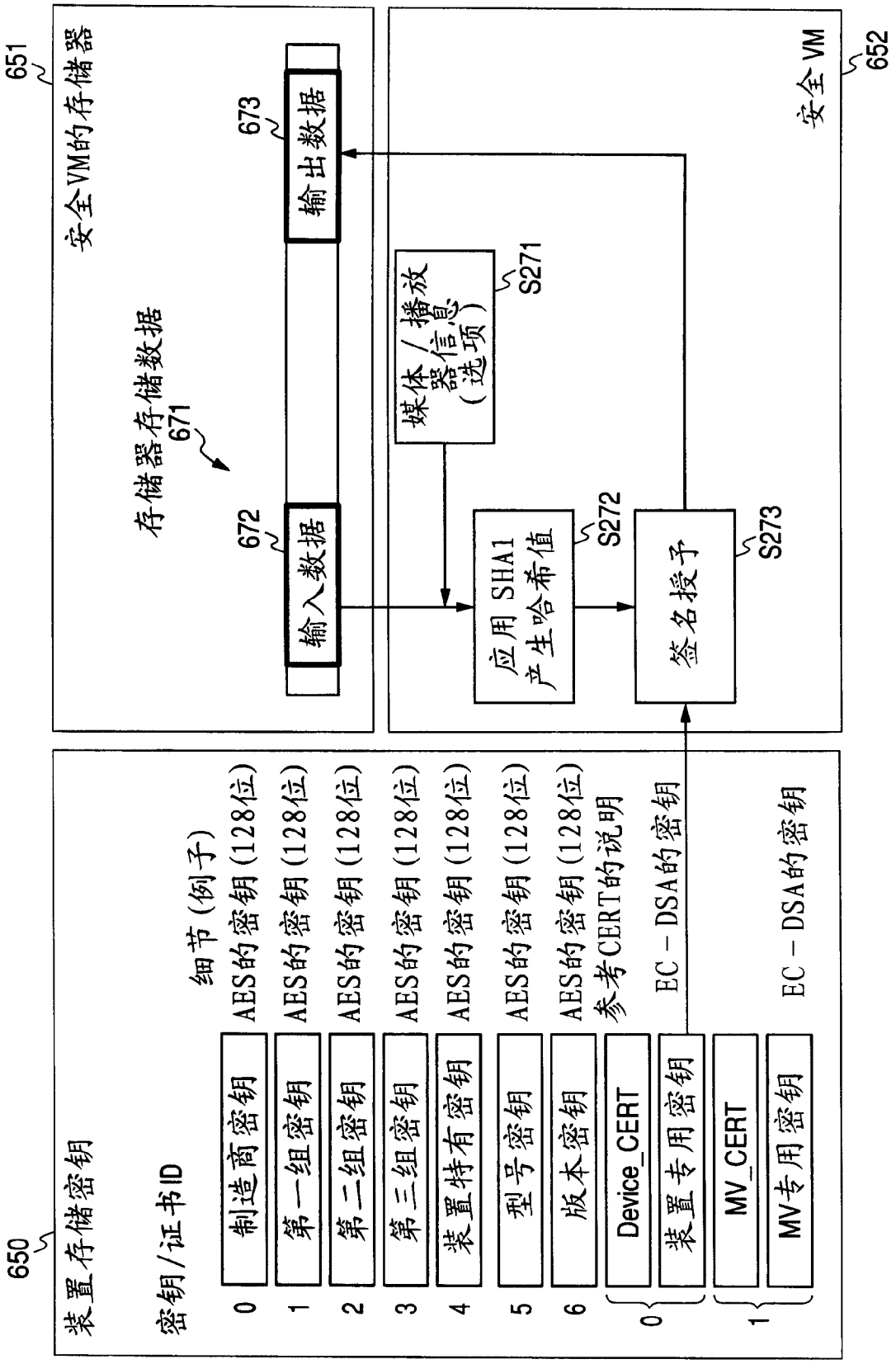

650
装置存储密钥
密钥/证书ID
细节（例子）
0 制造商密钥 AES的密钥（128位）
1 第一组密钥 AES的密钥（128位）
2 第二组密钥 AES的密钥（128位）
3 第三组密钥 AES的密钥（128位）
4 装置特有密钥 AES的密钥（128位）
5 型号密钥 AES的密钥（128位）
6 版本密钥 AES的密钥（128位）
0 Device_CERT 参考CERT的说明
装置专用密钥 EC－DSA的密钥
1 MV_CERT
MV专用密钥 EC－DSA的密钥
651
安全VM的存储器
存储器存储数据
671
672
输入数据
673
输出数据
媒体／播放器信息（选项）
S271
应用 SHA1 产生哈希值
S272
签名授予
S273
安全 VM
652

图 23

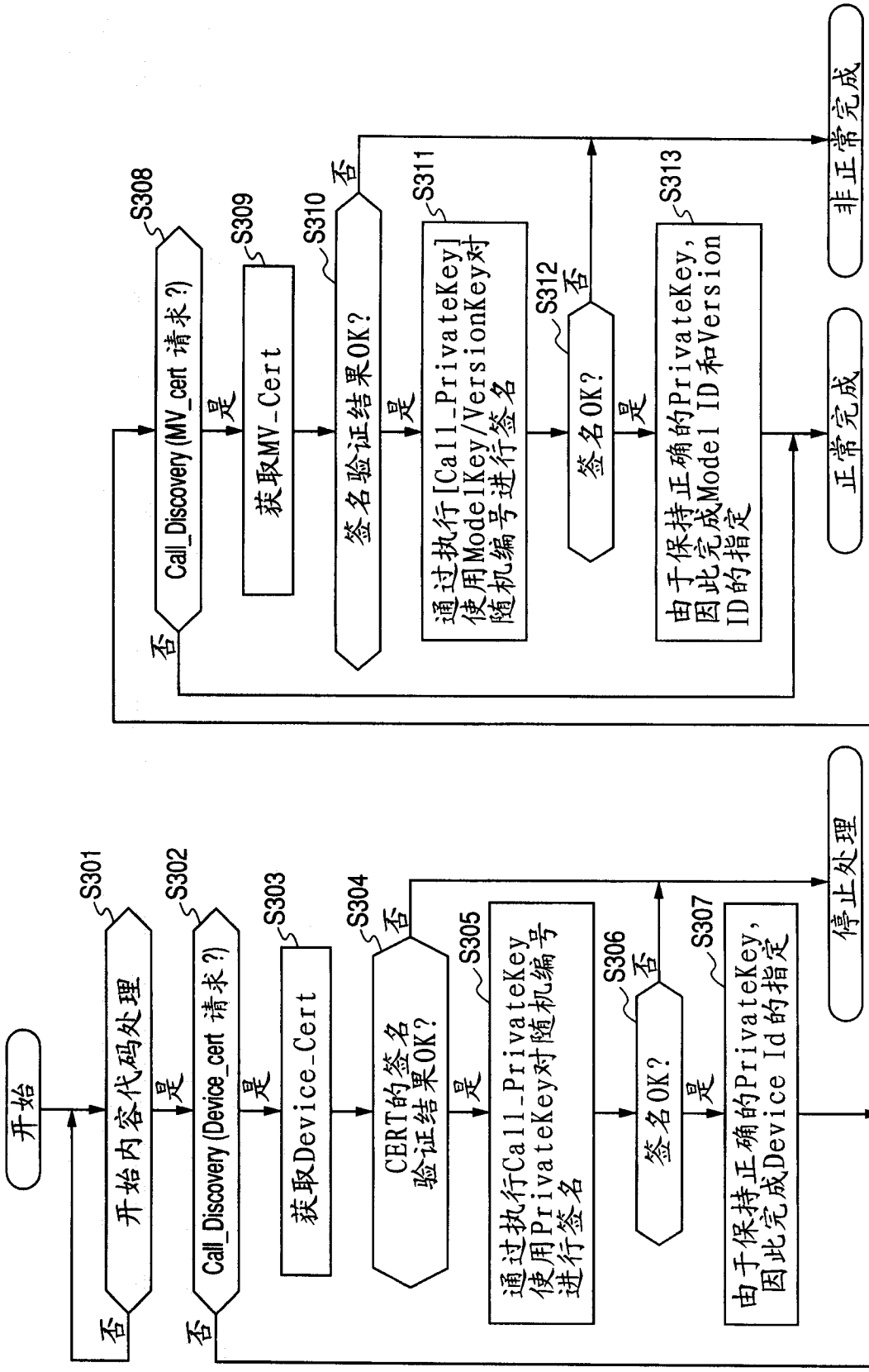

开始
S301
开始内容代码处理
否
是
S302
Call_Discovery (Device_cert 请求?)
否
是
S303
获取Device_Cert
S304
CERT的签名验证结果OK?
否
是
S305
通过执行Call_PrivateKey使用PrivateKey对随机编号进行签名
S306
签名OK?
否
是
S307
由于保持正确的PrivateKey，因此完成Device Id的指定
停止处理
S308
Call_Discovery (MV_cert 请求?)
否
是
S309
获取MV_Cert
S310
签名验证结果OK?
否
是
S311
通过执行[Call_PrivateKey]使用ModelKey/VersionKey对随机编号进行签名
S312
签名OK?
否
是
S313
由于保持正确的PrivateKey，因此完成Model ID和Version ID的指定
正常完成
非正常完成

图 24

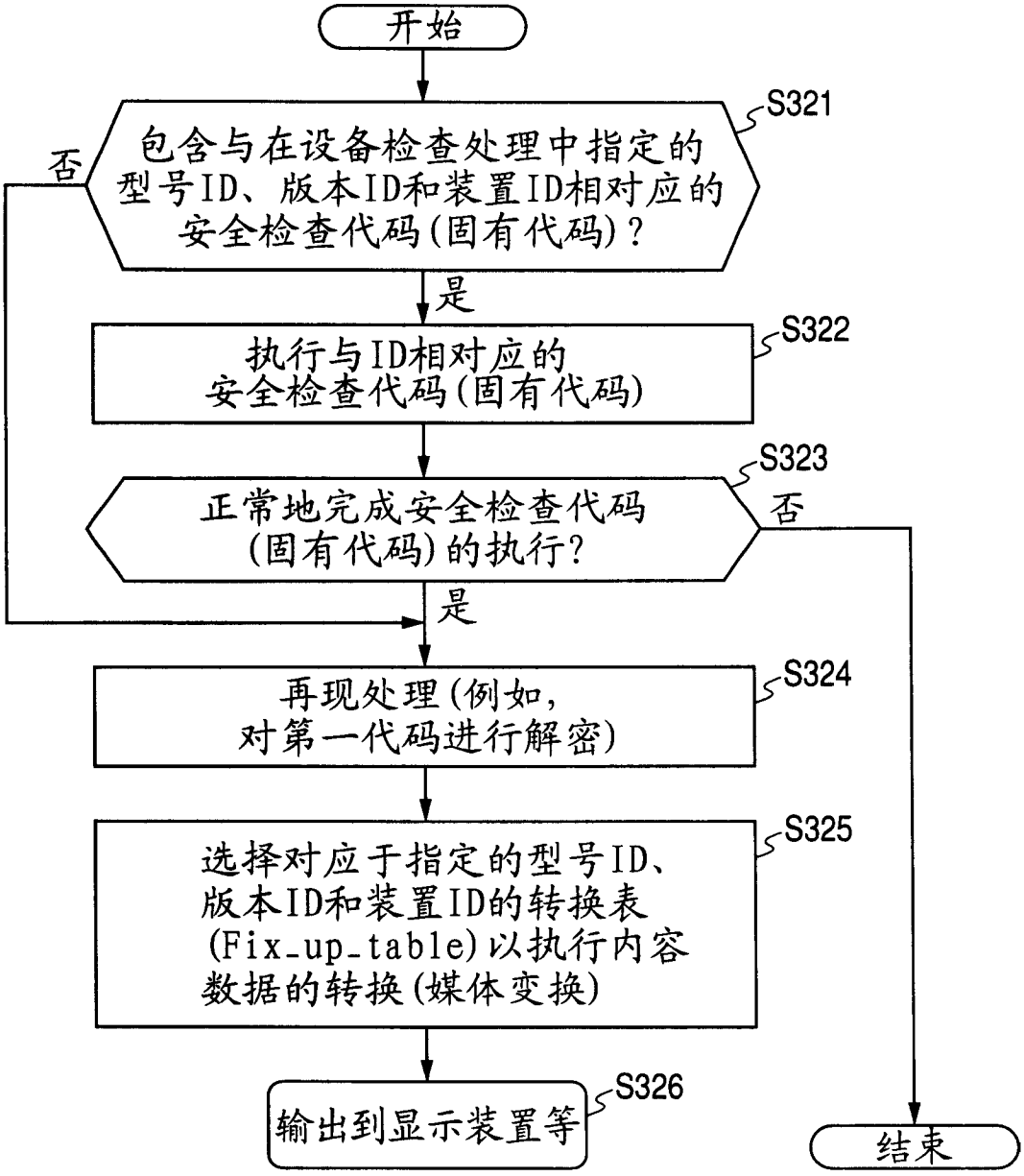

开始
S321
包含与在设备检查处理中指定的型号ID、版本ID和装置ID相对应的安全检查代码(固有代码)?
否
是
S322
执行与ID相对应的安全检查代码(固有代码)
S323
正常地完成安全检查代码(固有代码)的执行?
否
是
S324
再现处理(例如,对第一代码进行解密)
S325
选择对应于指定的型号ID、版本ID和装置ID的转换表(Fix_up_table)以执行内容数据的转换(媒体变换)
S326
输出到显示装置等
结束

图 25

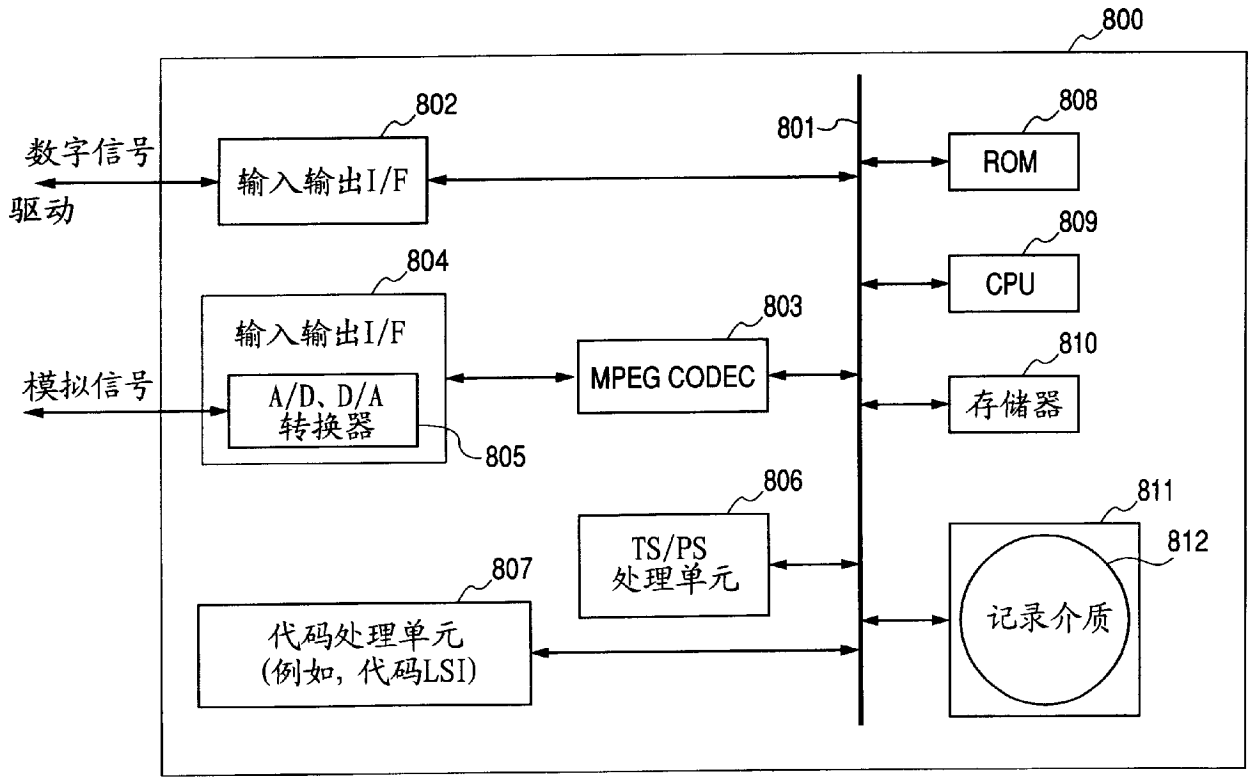

800
802
801
808
数字信号
驱动
输入输出I/F
ROM
809
CPU
804
803
输入输出I/F
MPEG CODEC
810
模拟信号
A/D、D/A
转换器
存储器
805
806
811
TS/PS
处理单元
812
807
记录介质
代码处理单元
(例如，代码LSI)

图 26

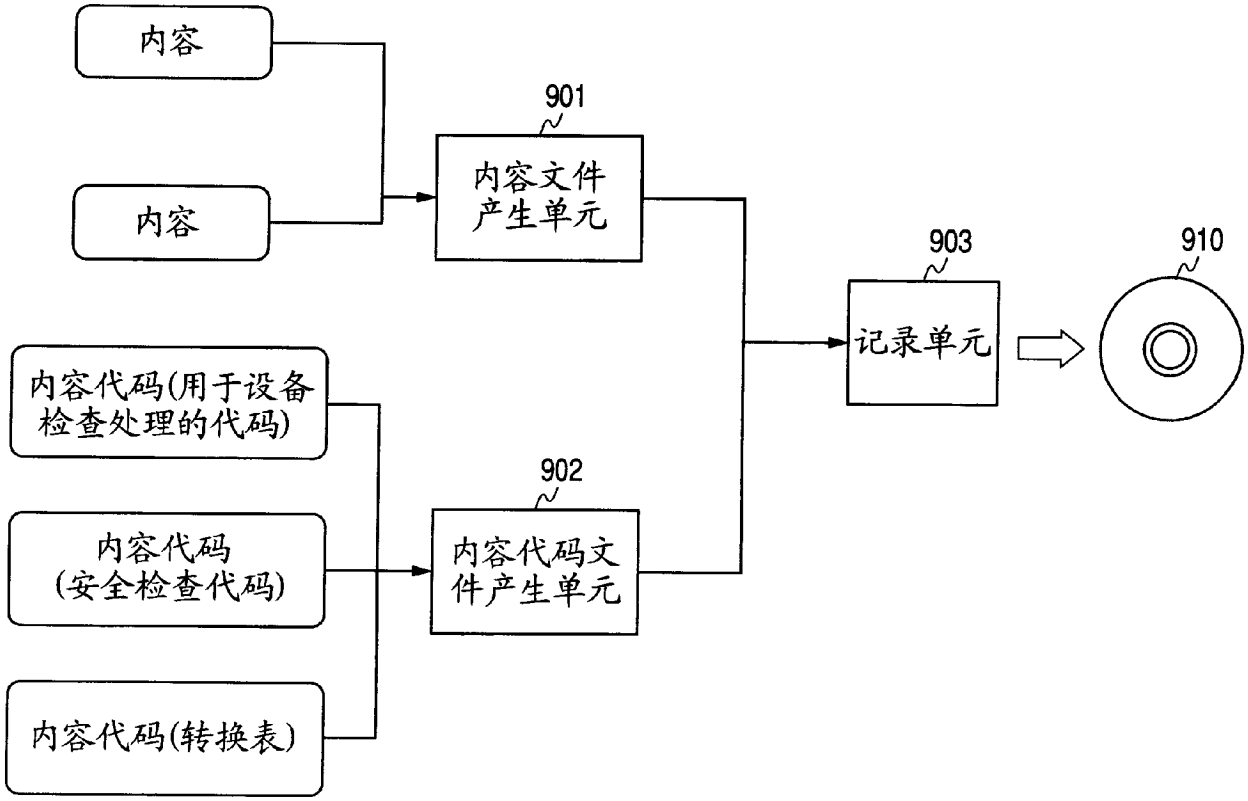

内容
内容
901
内容文件产生单元
903
记录单元
910
内容代码(用于设备检查处理的代码)
902
内容代码(安全检查代码)
内容代码文件产生单元
内容代码(转换表)

图 27