[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06F 1/00 (2006.01)
G11B 20/00 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510104138.7

[43] 公开日 2006 年 5 月 31 日

[11] 公开号 CN 1779689A

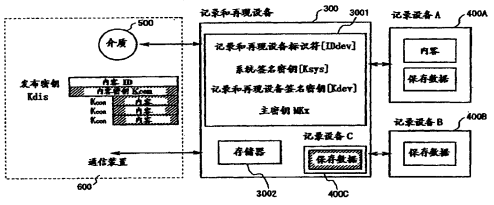
[22] 申请日 2001.1.19
[21] 申请号 200510104138.7
分案原申请号 02129853.X
[30] 优先权
[32] 2000.1.21 [33] JP [31] 13322/00
[32] 2000.1.25 [33] JP [31] 15551/00
[32] 2000.1.25 [33] JP [31] 15858/00
[32] 2000.1.25 [33] JP [31] 16029/00
[32] 2000.1.25 [33] JP [31] 16213/00
[32] 2000.1.25 [33] JP [31] 16251/00
[32] 2000.1.25 [33] JP [31] 16292/00
[71] 申请人 索尼公司
地址 日本东京都
共同申请人 索尼电脑娱乐公司
[72] 发明人 浅野智之 石桥义人 白井太三
秋下彻 吉森正治 田中诚
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 张志醒
权利要求书 5 页 说明书 150 页 附图 92 页

[54] 发明名称

数据处理设备和数据处理方法

[57] 摘要

本发明提供了一种能够确保保存数据安全的记录再现播放器和保存数据处理方法。保存数据被存储在记录装置中，利用程序的专用加密密钥，如内容密钥，或者基于内容密钥生成的保存数据加密密钥加密，以及当再现保存数据时，使用程序所特有的保存数据解密密钥，实施解密处理。而且，它还可能根据各种限制信息，生成存储数据加密密钥，比如通过利用记录再现播放器的专用密钥或者用户口令创建的保存数据加密和解密密钥，对保存数据实施解密和加密，实现保存数据的存储和再现。



1. 一种数据处理系统，包括用于在相互之间进行加密数据传输的记录装置和记录器/再现设备，其特征在于：

所述记录装置具有数据存储区域，用于存储可以在记录器/再现设备和记录装置之间传输的内容数据，同时，还具有多个密钥块，存储至少可适用于记录器/再现设备和记录装置之间的验证处理的密钥数据，以及存储在多个密钥块中的密钥数据有各个块存储不同的密钥数据的配置；

所述记录器/再现设备如下的配置：在记录器/再现设备与记录装置之间的验证处理中，从保存在所述记录装置中的多个密钥块中指定一个密钥块，根据存储在指定的密钥块内的密钥数据对所述记录装置实施验证处理。

2. 如权利要求 1 的数据处理系统，其特征在于，至少可适用于验证处理的验证密钥被包括在所述记录装置的多个密钥块的各个块中，各个密钥块的验证密钥被配置为各不相同的密钥数据。

3. 如权利要求 1 的数据处理系统，其特征在于具有以下配置：所述记录器/再现设备保存设置信息，其中，一个将应用验证处理的密钥块作为记录器/再现设备中的存储器内的指定的密钥块；和

所述记录器/再现设备，当要实施记录器/再现设备与记录装置之间的验证处理时，根据保存在记录器/再现设备中的存储器内的设置信息，从记录装置保存的多各密钥块中指定一个密钥块，并实施验证处理。

4. 如权利要求 3 的数据处理系统，其特征在于具有以下配置：所述记录器/再现设备的指定的密钥块设置信息，对各个预定的产品单元，如记录器/再现设备的型号、版本或发送目的地，被设定成是不同的。

5. 如权利要求 1 的数据处理系统，其特征在于：

所述记录器/再现设备具有以下配置：对所述记录装置进行验证处理所需要的验证处理密钥数据被存储在记录器/再现设备中的存储器内；和

存储在记录器/再现设备中的存储器内的验证处理密钥数据的验证，只建立在使用存储在所述记录装置中的多个密钥块内的部分块中

的密钥数据的密钥数据验证处理中，不能建立在使用其他密钥块内的密钥数据的验证处理中。

6. 如权利要求 1 的数据处理系统，其特征在于：

所述记录器/再现设备把用于记录装置验证密钥的主密钥 MKake 存储在记录器/再现设备的存储器内；和

根据所述用于记录装置验证密钥的主密钥 Mkake 生成的验证密钥是一个验证密钥，其验证只能建立在使用记录器/再现设备内指定的块所设置的密钥数据的验证处理中，不能建立在使用其它密钥块内的密钥数据的验证处理中。

7. 如权利要求 6 的数据处理系统，其特征在于：

所述记录装置配置成在所述记录装置内的存储器中的记录装置识别信息 IDmem 和，同时，各个密钥块之间不同的验证密钥 Kake 被存储在多个密钥块的各块中；和

所述记录器/再现设备配置成根据存储在记录器/再现设备存储器内的用于记录装置验证的主密钥 MKake，由记录装置识别信息 IDmem 的加密处理，生成验证密钥 Kake，并利用用验证密钥 Kake 生成的所述记录装置的指定的密钥块，进行验证处理。

8. 如权利要求 1 的数据处理系统，其特征在于，所述记录装置的各个密钥块包括，作为记录装置特有信息的记录装置标识符信息，验证密钥和将用于记录器/再现设备验证处理的的随机数生成密钥，以及将用于存储到所述存储单元的数据的加密处理的存储密钥。

9. 如权利要求 8 的数据处理系统，其特征在于：

存储在所述记录装置的多个密钥块的各块内的存储密钥是在各个块之间不同的密钥数据，同时是将用于所述数据存储单元的存储数据的进行加密处理的密钥；和

所述记录装置配置成执行记录装置中存储密钥的密钥交换处理，并且如果利用通过从记录装置外部所接收到的存储密钥加密的数据的请求，由不同于存储密钥的密钥把加密数据输出到记录装置外部。

10. 如权利要求 1 的数据处理系统，其特征在于：

所述记录装置具有加密处理单元；和

加密处理单元配置成根据从记录器/再现设备接收到的密钥块指

定信息，从记录装置的多个密钥块中选择一个密钥块，并利用所选择的密钥块内的密钥数据对所述记录器/再现设备进行验证处理。

11. 如权利要求 10 的数据处理系统，其特征在于，所述记录装置的加密处理单元配置成实施加密处理，加密处理是在存储可以在记录器/再现设备与记录装置之间传输的内容数据的数据存储单元内的数据存储处理，以及在数据存储单元的传输处理中进行的，并利用根据从记录器/再现设备接收到的密钥块指定信息而选择的一个密钥块中的密钥数据而进行的。

12. 如权利要求 1 的数据处理系统，其特征在于，在所述记录器/再现设备的所述记录装置中有多个可指定的密钥块，而且，在多个可指定的密钥块中至少有一个密钥块被配置为共同可指定的密钥块，它也可以在其它记录器/再现设备内被指定。

13. 一种记录装置，具有用来存储可以传输到外部设备的内容数据的数据存储单元，其特征是，配置成多个存储密钥数据的密钥块，至少可以适用于记录装置和所述外部装置之间的验证处理，以及存储在多个密钥块内的密钥数据配置成用于存储各块的密钥数据。

14. 如权利要求 13 的记录装置，其特征在于，所述记录装置的多个密钥块的各个密钥块包括至少可以适用于验证处理的验证密钥，以及各密钥块的验证密钥被配置成各不相同的密钥数据。

15. 如权利要求 13 的记录装置，其特征在于，所述记录装置配置成所述记录装置中的存储器具有记录装置识别信息 IDmem 和，同时，各密钥块的不同的验证密钥 Kake 被存储在多个密钥块的各块中。

16. 如权利要求 13 的记录装置，其特征在于，所述记录装置的各密钥块包括包括，作为记录装置特有信息的记录装置标识符信息，验证密钥和将用于所述外部装置的验证处理的随机数生成密钥，以及将用于把数据存储到所述存储单元的加密处理的存储密钥。

17. 如权利要求 16 的记录装置，其特征在于：

存储在所述记录装置的多个密钥块的各块内的存储密钥是在各个块之间不同的密钥数据，同时是将用于关于所述数据存储单元的存储数据的加密处理的密钥；和

所述记录装置配置成执行记录装置中存储密钥的密钥交换处理，并且如果利用通过从记录装置外部所接收到的存储密钥加密的数

据的请求，由不同于存储密钥的密钥把加密数据输出到记录装置外部。

18. 如权利要求 13 的记录装置，其特征在于：

所述记录装置具有加密处理单元；和

加密处理单元配置成根据从记录器/再现设备接收到的密钥块指定信息，从记录装置的多个密钥块中选择一个密钥块，并利用所选择的密钥块内的密钥数据对所述记录器/再现设备进行验证处理。

19. 如权利要求 18 的记录装置，其特征在于，所述记录装置的加密处理单元配置成实施加密处理，加密处理是在存储可以在外部装置与记录装置之间传输的内容数据的数据存储单元内的数据存储处理，以及在数据存储单元的传输处理中进行的，利用根据从外部装置接收到的密钥块指定信息所选择的一个密钥块中的密钥数据。

20. 一种数据处理系统中的数据处理方法，数据处理系统包含用于在相互之间传输加密数据的记录装置和记录器/再现设备，其特征在于，记录器/再现设备从记录装置所保存的多个密钥块中指定一个密钥块，并根据存储在所指定的密钥块内的密钥数据对记录装置进行验证处理。

21. 如权利要求 20 的数据处理方法，其特征在于，至少可以适用于验证处理的验证密钥被包括在所述记录装置的多个密钥块的各块中，并且各个密钥块的验证密钥被配置为各块之间各不相同。

22. 如权利要求 20 的数据处理方法，其特征在于，当要实施记录器/再现设备与记录装置之间的验证处理时，根据保存在记录器/再现设备中的存储器内的设置信息，所述记录器/再现设备从记录装置保存的多个密钥块中指定一个密钥块，并实施验证处理。

23. 如权利要求 20 的数据处理方法，其特征在于，所述记录器/再现设备把用于记录装置验证密钥的主密钥 MKake 存储在记录器/再现设备的存储器内，根据所述用于记录装置验证密钥的主密钥 Mkake 生成验证密钥 Kake，并利用记录装置所保存的指定的多个密钥块中的密钥块内的密钥数据，利用所生成的验证密钥 Kake，进行验证处理。

24. 如权利要求 20 的数据处理方法，其特征在于：

所述记录装置配置成在所述记录装置内的存储器中的记录装置识别信息 IDmem 和，同时，各个密钥块之间不同的验证密钥 Kake 被

存储在多个密钥块的各块中；和

通过根据存储在记录器/再现设备中的存储器内的用于记录装置验证的主密钥 MKake 加密所述记录装置识别信息 IDmem，所述记录器/再现设备生成验证密钥 Kake，并利用所生成的验证密钥 Kake 与所指定的所述记录装置的密钥块进行验证处理。

25. 如权利要求 20 的数据处理方法，其特征在于，记录装置根据从记录器/再现设备接收到的密钥块指定信息，从记录装置的多个密钥块中选择一个密钥块，并利用所选择的密钥块内的密钥数据对所述记录器/再现设备进行验证处理。

26. 如权利要求 20 的数据处理方法，其特征在于，所述记录装置实施加密处理，加密处理是在存储可以在记录器/再现设备与记录装置之间传输的内容数据的数据存储单元内的数据存储处理，以及在数据存储单元的传输处理中进行的，它利用根据从所述记录器/再现设备接收到的密钥块指定信息而选择的一个密钥块中的密钥数据而进行。

27. 如权利要求 20 的数据处理方法，其特征在于：

所述记录装置的多个密钥块的各块包括在所述记录装置内的数据存储单元的存储的数据的加密处理中使用的存储密钥；和

所述记录装置执行记录装置内存储密钥的密钥交换处理，并且如果利用通过从记录装置外部所接收到的存储密钥加密的数据的请求，通过不同于存储密钥的密钥把加密数据输出到记录装置外部。

28. 一种程序提供媒体，用于提供计算机程序，计算机程序使计算机系统在数据处理系统中实施数据处理方法，数据处理系统包括记录器/再现设备和记录装置，以执行相互之间的加密数据传输，其特征在于，所述计算机程序包括步骤：记录器/再现设备在由记录装置保存的多个密钥块内指定一个密钥块，并根据存储在所指定的密钥块内的密钥数据对记录装置进行验证处理。

数据处理设备和数据处理方法

本申请是申请日为2001年1月19日、申请号为02129853.X、发明名称为数据处理设备和数据处理方法的申请的分案申请。

技术领域

本发明涉及数据处理设备、数据处理方法，具体地说，本发明涉及一种用于验证构成数据内容的数据是否有效（即检查数据是否被篡改）的方法和设备以及一种用于给出验证值的方法，本发明还涉及能通过采用与其各自的密钥相对应的主密钥生成加密过程所需的各个不同密钥来增强安全性的设备和方法。而且，本发明能提供这样一种结构，它能排除对内容数据的非法使用，或者，更具体地说，本发明涉及能识别非法再现装置并排除非法使用所述内容的设备和方法。此外，本发明涉及能根据对数据处理设备所特定的信息很容易地将内容设置成仅能供使用内容数据的数据处理设备所用、和将内容数据设置成还能供其它处理设备所用的设备和方法。再有，本发明涉及到用于验证组构数据内容的数据的有效性（即验证存在或不存在篡改）的方法、设备和验证值给出方法。

此外，本发明涉及这样的数据处理设备、内容数据生成方法和数据处理方法，它们可实现一种内容数据结构，以便在这样一种结构中高度安全管理地提供和使用内容数据，在所述结构中，对包括声音信息、图像信息和节目数据之一的数据应用了加密处理，将所述数据连同多种头标信息提供给内容用户，并且，内容用户执行记录设备中的再现、执行或存储处理过程。

再有，本发明涉及这样的数据处理设备、数据处理方法和内容数据生成方法，它们用于提供一种结构，以便在数据内容是压缩的声音数据、图像数据和类似的数据的情况下提供能有效地执行再现处理过程，具体地说，上述数据处理设备、数据处理方法和内容数据生成方法用于形成这样一种内容数据的结构，其中，压缩数据和扩展处理程序结合在一起、根据压缩数据内容的头标信息来检索和抽取可应用的扩展处理程序，从而去执行再现处理过程，其中在所述头标信息中，所应用的扩展处理程序作为头标信息被存储。

再有，本发明涉及这样一种结构和方法，它用于再现诸如声音、图像、游戏或程序之类的各种内容，所说的内容可通过诸如 DVD 或 CD 之类的记录介质或诸如 CATV、因特网或卫星通信之类的有线或无线通信装置在用户所拥有的记录和再现设备中使用，并且，所述结构和方法可将内容存储到例如存储卡、硬盘或 CD-R 的排它性记录设备内，以便可实现这样的结构，它能在使用存储在记录设备中的内容时施加内容发布者所希望的使用限制并提供安全性，从而，所发布的内容不会被除合法用户以外的第三者非法使用。

背景技术

相关技术说明

目前通过诸如因特网之类的网络或通过诸如 DVD 或 CD 之类的可发布存储介质来发布诸如游戏程序、声音数据、图像数据或文档程序(在以下将这些称为“内容”)之类的数据。这些发布内容可存储在诸如存储卡或硬盘之类的记录设备内，所述记录设备可与用户拥有的诸如个人计算机(PC)或游戏装置之类的记录和再现设备相连接，因此，一经存储之后，所述内容就可从存储介质中再现出来。

诸如视频游戏设备或 PC 之类的通常信息设备中使用的存储卡的主要组件包括：连接装置，它用于对操作进行控制；连接器，它用于和一个槽相连，而所说的槽则与连接装置相连并被形成在信息设备上；非易失性存储器，它与控制装置相连，以便存储数据和其它内容。所述设置在存储卡中的非易失性存储器包括 EEPROM、闪存存储器或类似的存储器。

根据来自诸如游戏设备或 PC 之类的用作再现设备的信息设备主体的用户命令或者根据通过相连的输入装置提供的用户命令，从非易失性存储器中调用诸如数据或程序之类的存储在存储卡中的多种内容，这些内容可从信息设备主体或从与所述主体相连的显示器、扬声器或类似装置中再现。

诸如游戏程序、音乐数据或图像数据之类的多种软件内容一般具有由其创造者或销售者所持有的发布权。因此，在发布这些内容时，一般使用这样一种结构，它能施加专门的使用限制，也就是说，仅允许合法用户使用软件，从而能防止非法拷贝或类似操作，也就是说，考虑了安全性。

实现用户的使用限制的一种方法是这样一种过程，它用于对发布的内容进行加密。上述过程包括这样的装置，它用于例如通过因特网

发布诸如声音数据、图像数据或游戏程序之类的被加密了的多种内容并且对于被确认是合法用户的人对发布的加密内容进行解密，所述装置对应于用于施加解密钥的结构。

加密数据可以根据预定程序通过解密过程而返回到获得可用的解密数据(无格式文本)。这种为信息加密过程而使用加密密钥同时为解密过程而使用解密密钥的数据加密和解密方法通常是周知的。

存在有多种类型的使用加密密钥和解密密钥的数据加密和解密的方法，一个实例称为共用密钥密码系统。共用密钥密码系统使用一种用于数据加密过程的共用加密密钥以及一种用于数据解密过程的共用解密密钥，并将这些供加密和解密过程使用的共用密钥告知合法用户，同时拒绝无密钥的非法用户的数据访问。这种密码系统的代表性实例是 DES(数据加密标准)。

例如可通过根据口令或类似内容应用诸如散列（hash）函数之类的单向函数而获得供加密和解密过程使用的加密和解密密钥。单向函数难以从其输出确定其输入。例如，将用户所决定的口令用作输入以便应用一单向函数，从而根据该函数的输出生成加密和解密密钥。根据这样获得到加密和解密密钥来确定作为密钥的原始数据的口令是基本上不可能的。

此外，称为“公共密钥密码系统”的方法针对供加密用的加密密钥为基础的过程和供解密用的解密密钥为基础的过程而使用了不同的算法。公共密钥密码系统使用了可为非指定用户使用的公共密钥，因此，可用特定用户发出的公共密钥来对用于该特定用户的加密文档进行解密。用公共密钥加密的文档只能用与供解密过程使用的公共密钥相对应的密钥来解密。由于所述密钥为业已发出公共密钥的个人所拥有，故用公共密钥加密的文档只能由具有该密钥的个人来解密。代表性的公共密钥密码系统是 RSA(Rivest-shamir-Adleman)加密。

使用这种密码系统可以使得加密的内容仅对合法用户解密。以下参照图 1 简要说明使用这种密码系统的通常内容发布结构。

图 1 示出了诸如 PC(个人计算机)或游戏设备之类的再现装置 10 再现从诸如 DVD、CD30 或因特网 40 之类的数据提供装置中获得的程序、声音或视频数据或类似数据(内容)的结构的一个实例，其中，获得来自 DVD、CD30、因特网 40 或类似装置的数据被存储在诸如软盘、存储

卡、硬盘或类似设备之类的存储装置 20 内。

将诸如程序、声音或视频数据之类的内容提供给具有再现装置 10 的用户。合法用户获得加密数据和密钥数据，该密钥数据是加密和解密密钥。

再现装置 10 具有 CPU12，以便通过再现处理部 14 再现输入数据。再现处理部 14 对加密数据进行解密，以便再现所提供的程序和诸如声音或图像数据之类的内容。

合法用户将诸如程序和数据之类的内容保存在存储装置 20 内，以便再次使用所提供的程序。再现装置 10 具有保存处理部 13，它用于执行上述内容保存过程。保存处理部 13 对数据进行加密和保存，以便防止存储在存储装置 20 内的数据被非法使用。

用内容加密密钥去对内容进行加密。保存处理部 13 使用内容加密密钥去对内容进行加密，然后将加密的内容存储在诸如 FD(软盘)、存储卡或硬盘之类的存储装置 20 的存储部 21 内。

为了从存储装置 20 中获得并再现所存储的内容，用户从存储装置 20 中获得加密数据并使得再现装置 10 的再现处理部 14 用内容解密密钥即解密密钥去执行解密过程，以便从加密数据中获得并再现解密数据。

依照图 1 所示结构的通常实例，在诸如软盘或存储卡之类的存储装置 20 中对所存储的内容加密，从而，所述内容不能在外部读取。但是，当软盘要由诸如 PC 或游戏设备之类的另一信息设备的再现装置来再现时，再现是不可能的，除非是该再现装置具有相同的内容密钥即用于对加密内容进行解密的同样的解密密钥。因此，为了实现对多个信息设备都可用的形式，必须将共用的解密密钥提供给用户。

但是，使用共用内容加密密钥，意味着有较大可能性地以混乱的方式将加密处理密钥发给不具有合法许可的用户。因此，不能防止不具有合法许可的用户非法使用内容，并且难以拒绝在不具有合法许可的 PC、游戏设备或类似设备中进行非法使用。

在密钥信息从设备之一中泄漏的情况下，使用共用内容加密密钥和解密密钥会破坏利用上述密钥的整个系统。

此外，在使用上述共用密钥的环境中，可以很容易地例如将在某一 PC 上形成的并保存在诸如存储卡或软盘之类的存储装置中的内容拷

贝至另一软盘上。因此，利用拷贝的软盘而不是原始内容的使用形式是可能的，所以，会形成或篡改大量对诸如游戏设备或 PC 之类的信息设备可用的拷贝内容。

通常使用这样的方法，该方法包括验证内容数据中的完整性检查值，以便检查数据的有效性即是否有数据被篡改，然后，所述方法使记录和再现装置去比较根据要加以验证的数据所生成的整体性检查值与被包含在内容数据中的整体性检查值，以便对数据进行验证。

但是，用于数据内容的整体性检查值一般是为整个数据而生成的，并且为了比较这个为整个数据而生成的整体性检查值，就需要一个要加以检查的、为整个数据而生成的整体性检查值。例如如果一个整体性检查值 ICV 要用按 DES-CBC 模式生成的消息鉴别码(MAC)来确定，则必须对整个数据执行 DES CBC 过程。这种计算量会随数据的长度而线性地增加，从而以不利的方式减少处理效率。

发明内容

本发明解决了传统技术中的上述问题，作为本发明的第一个目的，是提供一种数据处理设备和方法以及数据验证值给出方法，所述设备和方法能有效地确认数据的有效性，并能有效地执行在验证之后执行的用于记录设备的下载过程、在验证之后执行的再现过程以及其它过程，此外，还提供了供上述设备和方法使用的程序提供介质。

此外，作为可用于将内容数据的使用限于授权用户的技术，可使用诸如数据加密、数据解密、数据验证、签名处理之类的多种加密处理过程。但是，执行这些种类的加密过程需要共用的秘密信息，例如用于对内容数据加密和解密的密钥信息或用于在两个设备即在其间传送内容数据的设备、或在其间执行鉴别处理的设备之间要加以共享的用于鉴别的鉴别密钥。

所以，在作为共享的秘密信息的密钥数据从两个设备之一中泄露的情况下，用上述共享密钥信息的内容加密数据可被没有许可的第三方解密，从而能非法地使用该内容。对泄露了鉴别密钥的情况来说也是一样，这就会导致在没有许可的情况对设备进行鉴别。所以，泄露密钥会因此而威胁整个系统。

本发明要解决上述问题。本发明的第二个目的是提供一种加密处理过程中的具有增强安全性的数据处理设备、数据处理系统和数据处

理方法。本发明的数据处理设备不将执行诸如数据加密、数据解密、数据验证、鉴别处理和签名处理之类的加密处理过程所需的各个密钥存储在存储部内，相反，将主密钥存储起来以便在存储部中生成上述各个密钥，并使加密处理部根据主密钥和所述设备或数据生成必要的各个密钥。

此外，可以通过使内容数据加密而保持一定程度的安全性。但是，在通过非法读取存储器而读出存储在存储器内的各加密密钥的情况下，密钥数据等会被泄露并在没有任何授权许可的情况下被拷贝到记录器/再现器上，以及可利用被拷贝的密钥信息而非法地使用内容。

本发明的第三个目的是提供一种具有能拒绝非法使用的结构（即能识别非法再现者并不允许被识别的再现者执行诸如再现和下载内容数据的结构）的形式的数据处理设备、数据处理方法和内容数据生成方法。

此外，可将内容数据的使用限于授权用户的技术包括用预定的加密密钥例如签名处理来进行加密处理。但是，传统的用签名的加密处理一般具有为所有使用系统中内容的实体所共有的签名密钥，这种签名密钥允许不同的设备使用共有的内容，这就有导致非法拷贝内容的问题。

可以存储利用唯一的口令加密的内容，但是该口令会被窃取，也可以通过不同的再现设备输入相同口令来解密同一个加密的内容，但是并不易于使得传统的安全结构去实施这样一种系统，该系统可识别一个重现设备以便只允许该重现设备使用所述内容。

业已实现了本发明以解决先有技术的上述问题，本发明的第四个目的是提供这样一种数据处理设备和数据处理方法，它能根据内容使用限制通过有选择地使用数据处理设备所专用的设备专用密钥和其它数据处理设备所共用的系统共用密钥而仅允许专门的数据处理设备再现内容。

再有，存在有作为将对内容数据的使用限于授权用户的方法而对内容数据进行加密处理。但是，有诸如声音信息、图像信息和程序数据之类的多种内容数据，并且，存在有诸如所有内容数据都需加密的情况和部分需要加密处理而部分不需要加密处理相混合的情况之类的情况下的多种内容。

对这些内容实施统一加密处理会产生内容再现处理过程中的不必要的解密处理，或者会就处理效率和处理速度而言会产生不利的环境。例如，就诸如实时再现是关键的音乐数据之类的数据而言，应该具有这样的内容数据结构，它可高速地应用解密处理过程。

本发明解决这些问题。本发明的第五个目的是提供这样一种数据处理设备、内容数据生成方法和数据处理方法，它能应用于与内容数据类型相对应的多种内容数据结构即与内容相对应的不同数据格式，并且能生成和处理在再现、执行等中具有高安全性和易于使用的内容数据。

此外，需要将解密的声音数据、图像数据和类似数据输出给 AV 输出部，以便再现。目前，多种内容在许多时候都是压缩的并存储在存储介质内或进行发布。所以，必须在再现之前扩展压缩数据。例如，如果声音数据是按 MP-3 方式压缩的，则用 MP3 解码器对声音数据进行解密，以便输出。如果内容数据是按 MP-3 方式压缩的图像数据，则用 MPEG2 解码器对声音数据进行扩展，以便输出。

但是，由于存在有多种压缩处理过程和扩展处理程序，所以，即使压缩数据是由内容提供商通过媒体或网络提供的，也不可能用不具有兼容扩展程序的再现设备来再现数据。

本发明的第六个目的是提供一种用于有效地执行已压缩数据的再现处理过程的结构，也就是说，本发明的第六个目的是提供一种数据处理设备、一种数据处理方法和一种内容数据生成方法，它们用于在内容是已压缩声音数据、图像数据或类似数据的情况下有效地执行再现处理过程。

通过提供一种数据处理设备和一种数据处理方法可达到本发明的上述目的和其它目的。

本发明的第一个方面是：用于对记录或通信介质提供的内容数据进行处理的数据处理设备，其特征在于，所述设备包括：密码翻译处理部，它用于对内容数据进行密码翻译处理；以及，控制部，它用于对密码翻译处理部进行控制，所述密码翻译处理部配置成：能生成作为整体性检查值的部分整体性检查值，它用于部分数据集，该数据集将内容数据构成部获得的一个或多个部分数据包含进多个部分；比较生成的整体性检查值以便验证该部分数据；根据包含至少一个或多个

部分整体性检查值的部分整体性检查数值集数据串生成中间整体性检查值；以及，使用所生成的中间整体性检查值去验证与构成部分整体性检查数值集的多个部分整体性检查值相对应的多个部分数据集的全部。

此外，本发明的数据处理设备的一个实施例的特征在于，通过密码翻译处理过程利用提供给它的部分检查值生成密钥生成部分整体性检查值，从而将要加以检查的部分数据用作一消息，通过密码翻译处理过程利用提供给它的总体检查值生成密钥生成中间整体性检查值，从而将要加以检查的部分整体性检查数值集数据串用作一消息，并且，所述密码翻译处理部配置成能存储部分整体性检查值生成值以及总体整体性检查值生成密钥。

再有，本发明的数据处理设备的一个实施例的特征在于，所述密码翻译处理过程具有与所生成的部分整体性检查值相对应的多种类型的部分检查值生成密钥。

再有，本发明的数据处理设备的一个实施例的特征在于，所述密码翻译处理过程是 DES 密码翻译处理过程，并且，所述密码翻译处理部配置成能执行 DES 密码翻译处理过程。

此外，本发明的数据处理设备的一个实施例的特征在于，作为消息的所述部分整体性检查值，是一个在 DES-CBC 模式下用要加检查的部分数据生成的消息鉴别码(MAC)，作为消息的所述中间值，是一个在 DES-CBC 模式下用要加检查的部分整体性检查数值集数据串生成的消息鉴别码(MAC)，并且，所述密码翻译处理部配置成能在 DES-CBC 模式下执行 DES 密码翻译处理过程。

再有，本发明的数据处理设备的一个实施例的特征在于，在密码翻译处理部的以 DES-CBC 模式为基础的密码翻译处理结构中，仅在要加以处理的消息串的一部分中应用三重 DES。

另外，本发明的数据处理设备的一个实施例的特征在于，所述数据处理设备具有一签名密钥，所述密码翻译处理部配置成能将一个通过签名密码应用翻译处理过程根据前述中间值生成的值用作数据验证的比较值。

再有，本发明的数据处理设备的一个实施例的特征在于，所述数据处理设备具有作为签名密钥的多个不同签名密钥，所述密码翻译处

理部配置成能将根据内容数据的位置选定的多个不同签名密钥之一用于对中间整体性检查值的密码翻译处理过程，以便获得数据验证用的比较值。

再有，本发明的数据处理设备的一个实施例的特征在于，所述数据处理设备具有为用于执行数据验证过程的系统的所有实体所共用的共用签名以及为执行数据验证过程的各设备所专用的设备专用签名。

再有，本发明的数据处理设备的一个实施例的特征在于，所述部分整体性检查值包含有为部分地构成数据的内部头标部数据而生成的一个或多个头标部整体性检查值、以及为部分地构成数据的内容块数据而生成的一个或多个内容整体性检查值，所述密码翻译处理过程配置成：能生成用于内部头标部数据中部分数据集的一个或多个头标部整体性检查值，以便去执行比较处理；生成用于内部内容部数据中部分数据集的一个或多个内容整体性检查值，以便去执行比较处理；以及，根据所生成的所有头标部整体性检查值和内容整体性检查值去生成总体整体性检查值，以便执行比较处理，从而对数据进行验证。

还有，本发明的数据处理设备的一个实施例的特征在于，所述部分整体性检查值包含有为部分地构成数据的内部头标部数据而生成的一个或多个头标部整体性检查值，所述密码翻译处理过程配置成：能生成用于内部头标部数据中部分数据集的一个或多个头标部整体性检查值，以便执行比较处理；以及，根据所生成的一个或多个头标部整体性检查值并根据构成一部分数据的内容块数据生成总体整体性检查值，以便执行比较处理，从而对数据进行验证。

再有，本发明的数据处理设备的一个实施例的特征在于，该设备还包括一记录设备，它用于存储密码翻译处理部所确认的数据。

此外，本发明的数据处理设备的一个实施例的特征在于，所述控制部配置成如果在密码翻译处理部所执行的过程中要比较部分整体性检查值，则不确立该比较，并且，所述控制部将用于把数据存储在记录设备中的过程挂起。

再有，本发明的数据处理设备的一个实施例的特征在于，该设备还包括一再现过程处理部，它用于再现由密码翻译处理部确认的数据。

此外，本发明的数据处理设备的一个实施例的特征在于，如果在

密码翻译处理部所执行的过程中要比较部分整体性检查值，则不确立该比较，并且，所述控制部将再现处理部中的再现过程挂起。

再有，本发明的数据处理设备的一个实施例的特征在于，该设备包括控制装置，它用于在密码翻译处理部所执行的比较部分整体性检查值的过程中仅比较数据中的头标部整体性检查值，并将业已为其进行了头标部整体性检查值的比较的数据传送给用于再现的再现处理部。

而且，本发明的第二个方面是用于对记录或通信介质提供的内容数据进行处理的数据处理设备，其特征在于，所述设备包括：密码翻译处理部，它用于对内容数据进行密码翻译处理；以及，控制部，它用于对密码翻译处理部进行控制，所述密码翻译处理部配置成：若对要加以验证的数据进行加密，则能通过签名数据应用密码翻译处理过程根据因对解密数据执行算法操作过程而获得的算法操作结果来从数据中生成用于要加以验证的数据的整体性检查值，其中所述解密数据则是通过对加密数据执行解密处理过程而获得的。

此外，本发明的数据处理设备的一个实施例的特征在于，所述算法操作过程包括对解密数据每隔预定字节都执行异或操作，所述解密数据是通过对加密数据进行解密而获得的。

而且，本发明的第三实施例是一种数据处理方法，它用于处理通过记录或通信介质提供的内容数据，所述方法的特征在于，该方法：能生成作为整体性检查值的部分整体性检查值，它用于部分数据集，该数据集将内容数据构成部获得的一个或多个部分数据包含进多个部分；比较生成的整体性检查值以便验证该部分数据；根据包含至少一个或多个部分整体性检查值的部分整体性检查数值集数据串生成中间整体性检查值；以及，使用所生成的中间整体性检查值去验证与构成部分整体性检查数值集的多个部分整体性检查值相对应的多个部分数据集的全部。

此外，本发明的数据处理方法的一个实施例的特征在于，通过密码翻译处理过程利用提供给它的部分检查值生成密钥生成部分整体性检查值，以便将要加以检查的部分数据用作一消息，通过密码翻译处理过程利用提供给它的部分检查值生成密钥生成中间整体性检查值，以便将要加以检查的部分整体性检查数值集数据串用作一消息。

再有，本发明的数据处理方法的一个实施例的特征在于，通过应用与所生成的部分整体性检查值相对应的不同类型的部分检查值部生成整体性检查值。

再有，本发明的数据处理方法的一个实施例的特征在于，所述密码翻译处理过程是 DES 密码翻译处理过程。

此外，本发明的数据处理方法的一个实施例的特征在于，所述部分整体性检查值作为消息是在 DES-CBC 模式下用要加检查的部分数据生成的消息鉴别码(MAC)，所述中间值作为消息是在 DES-CBC 模式下用要加检查的部分整体性检查数值集数据串生成的消息鉴别码(MAC)。

另外，本发明的数据处理方法的一个实施例的特征在于，将通过签名密钥应用翻译处理过程根据前述中间值生成的值用作数据验证的比较值。

再有，本发明的数据处理方法的一个实施例的特征在于，根据内容数据的位置将不同的签名密钥应用于用于中间整体性检查值的密码翻译处理过程，以便获得数据验证用的比较值。

再有，本发明的数据处理方法的一个实施例的特征在于，选定为用于执行数据验证过程的系统的所有实体所共用的共用签名密钥或为执行数据验证过程的各设备所专用的设备专用签名密钥并根据内容数据的位置将它们用作签名密钥。

再有，本发明的数据处理方法的一个实施例的特征在于，所述部分整体性检查值包含有为部分地构成数据的内部头标部数据而生成的一个或多个头标部整体性检查值以及为部分地构成数据的内部内容部数据而生成的一个或多个内容整体性检查值，数据验证处理过程：能生成用于内部头标部数据中部分数据集的一个或多个头标部整体性检查值，以便执行比较处理；生成用于内部内容部数据中部分数据集的一个或多个内容整体性检查值，以便执行比较处理；以及，根据所生成的所有头标部整体性检查值和内容整体性检查值生成总体整体性检查值，以便执行比较处理，从而对数据进行验证。

还有，本发明的数据处理方法的一个实施例的特征在于，所述部分整体性检查值包含有为部分地构成数据的内部头标部数据而生成的一个或多个头标部整体性检查值，所述数据验证处理过程包括：能生成用于内部头标部数据中部分数据集的一个或多个头标部整体性检查

值，以便执行比较处理；以及，根据所生成的一个或多个头标部整体性检查值并根据构成一部分数据的内容块数据生成总体整体性检查值，以便执行比较处理，从而对数据进行验证。

再有，本发明的数据处理方法的一个实施例的特征在于，该方法还包括一用于存储的处理过程，该过程在数据验证之后存储所确认的数据。

此外，本发明的数据处理方法的一个实施例的特征在于，如果是在用于比较部分整体性检查值的过程中，则不确立该比较，并且，进行控制以便将用于把数据存储在记录设备中的过程挂起。

再有，本发明的数据处理方法的一个实施例的特征在于，该方法还包括一再现处理过程，它用于在数据确认之后再现数据。

此外，本发明的数据处理方法的一个实施例的特征在于，如果是在用于比较部分整体性检查值的过程中，则不确立该比较，进行控制以便将再现处理部中执行的再现过程挂起。

再有，本发明的数据处理方法的一个实施例的特征在于，该方法在用于比较部分整体性检查值的过程中仅比较数据中的头标部整体性检查值并将业已为其进行了头标部整体性检查值的比较的数据传送给用于再现的再现处理部。

而且，本发明的第四个方面是用于对记录或通信介质提供的内容数据进行处理的数据处理方法，其特征在于，所述方法：若对要加以验证的数据进行加密，对通过对加密数据进行解密而获得的解密数据执行算法操作过程；根据算法操作过程所获得的算法操作结果对数据执行签名密钥应用密码翻译处理，以便生成用于要加以验证的数据的整体性检查值。

此外，本发明的数据处理方法的一个实施例的特征在于，所述算法操作过程包括对解密数据每隔预定字节都执行异或操作，所述解密数据是通过对加密数据进行解密而获得的。

而且，本发明的第五个方面是用于数据验证过程的数据验证值给出方法，其特征在于，所述方法：给出作为整体性检查值的部分整体性检查值，它用于部分数据集，该数据集将内容数据构成部获得的一个或多个部分数据包含进多个部分；以及，将一中间整体性检查值赋给要加以验证的数据，所述中间整体性检查值用于验证包含至少一个

或多个部分整体性检查值的部分整体性检查数值集数据串。

此外，本发明的数据验证值给出方法的一个实施例的特征在于，通过密码翻译处理过程利用提供给它的部分检查值生成密钥生成部分整体性检查值，以便将要加以检查的部分数据用作一消息，通过密码翻译处理过程利用提供给它的总体检查值生成密钥生成中间整体性检查值，以便将要加以检查的部分整体性检查数值集数据串用作一消息。

再有，本发明的数据处理设备的一个实施例的特征在于，通过应用与所生成的部分整体性检查值相对应的不同类型的部分检查值生成密钥来生成部分整体性检查值。

再有，本发明的数据验证值给出方法的一个实施例的特征在于，所述密码翻译处理过程是 DES 密码翻译处理过程。

此外，本发明的数据验证值给出方法的一个实施例的特征在于，所述部分整体性检查值作为消息是在 DES-CBC 模式下用要加检查的部分数据生成的消息鉴别码(MAC)，所述中间值作为消息是在 DES-CBC 模式下用要加检查的部分整体性检查数值集数据串生成的消息鉴别码(MAC)。

另外，本发明的数据验证值给出方法的一个实施例的特征在于，通过签名密钥应用密码翻译处理过程从中间值生成的值可用作数据验证的比较值。

再有，本发明的数据验证值给出方法的一个实施例的特征在于，根据内容数据的位置将不同的签名密钥应用于用于中间整体性检查值的密码翻译处理过程，以便获得数据验证用的比较值。

再有，本发明的数据验证值给出方法的一个实施例的特征在于，选定为用于执行数据验证过程的系统的所有实体所共用的共用签名以及为执行数据验证过程的各设备所专用的设备专用签名并根据内容数据的位置将其用作签名密钥。

再有，本发明的数据验证值给出方法的一个实施例的特征在于，所述部分整体性检查值包含有用于部分地构成数据的内部头标数据的一个或多个头标部整体性检查值以及用于部分地构成数据的内部内容部数据的一个或多个内容整体性检查值，所述方法设置成能生成用于所有头标部整体性检查值以及内容整体性检查值的总体整体性检查

值，以便对数据进行验证。

还有，本发明的数据验证值给出方法的一个实施例的特征在于，所述部分整体性检查值包含有用于部分地构成数据的内部头标数据的一个或多个头标部整体性检查值，所述方法配置成能生成用于一个或多个头标部整体性检查值和部分地构成数据的内容块数据的总体整体性检查值，以对数据进行验证。

而且，本发明的第六个方面是一种程序提供介质，它用于提供计算机程序，该程序用于在计算机系统上执行数据验证过程以便验证数据是有效的，所述程序提供介质的特征在于，所述计算机程序包括下列步骤：利用作为整体性检查值而生成的部分整体性检查值来执行比较过程，所述部分整体性检查值用于部分数据集，该数据集包含通过将数据划分成多个部分而获得的一个或多个部分数据；以及，用中间整体性检查值去验证与构成部分整体性检查数值集的多个部分整体性检查值相对应的多个部分数据集的全部，该中间整体性检查值建立在通过将多个部分整体性检查值结合到一起而获得的部分整体性检查值集的基础上。

本发明的第七个方面是一种数据处理设备，该设备包括：加密处理部，它执行数据加密、数据解密、数据验证、鉴别处理和签名处理中至少一个的加密处理；以及，存储部，它存储主密钥以便生成用于加密处理的密钥，所述设备的特征在于，上述加密处理部配置成能根据主密钥和所述设备的标识数据或经历加密处理的数据生成执行加密处理所必需的各个密钥。

依照本发明数据处理设备的另一个实施例，所述数据处理设备是这样一种数据处理设备，它对通过记录介质或通信介质对传输数据执行加密处理，所述设备的特征在于，上述存储部存储发布密钥生成主密钥 Mkdis，以便生成一发布密钥 kdis，此密钥用于对传送数据进行加密处理，所述加密处理部根据存储在存储部中的上述发布密钥生成主密钥 MKdis 和一是传送数据的标识数据的数据标识符执行加密处理过程并生成传输数据发布密钥 Kdis。

此外，依照本发明数据处理设备的另一个实施例，该数据处理设备是这样一种数据处理设备，它对向/从其传送数据的在外部连接的设备作鉴别处理，所述数据处理设备的特征在于，前述存储部存储有鉴

别密钥生成主密钥 Mkake，它用于生成外部连接的设备的鉴别密钥 Kake，所述加密处理部根据存储在存储部中的鉴别密钥生成主密钥以及是外部连接的设备的标识数据的外部连接设备的标识符执行加密处理并生成外部连接的设备的鉴别密钥 Kake。

再有，依照本发明数据处理设备的又一个实施例，该数据处理设备是这样一种数据处理设备，它对数据执行签名处理，所述数据处理设备的特征在于，前述存储部存储有签名密钥生成主密钥 Mkdev，它用于生成数据处理设备的数据处理设备签名密钥 kdev，所述加密处理部根据存储在存储部中的签名密钥生成主密钥 Mkdev 以及是数据处理设备的标识数据的数据处理设备的标识符执行加密处理并生成数据处理设备的数据处理设备签名密钥 Kdev。

此外，依照本发明数据处理设备的还一个实施例，根据主密钥和经历加密处理的设备或数据的标识数据而生成执行加密处理所必需的个别密钥的个别密钥生成处理过程是这样的加密处理过程，它将经历加密处理的设备或数据的标识数据的至少一部分用作消息并将主密钥用作加密密钥。

此外，依照本发明数据处理设备的又一个实施例，所述加密处理过程是用 DES 算法的加密处理过程。

再有，本发明的第八个方面是一种数据处理系统，它是由多个数据处理设备配置而生成，所述系统的特征在于，多个数据处理设备中的每一个设备都具有一共用主密钥，以生成用于数据加密、数据解密、数据验证、鉴别处理和签名处理中至少一个的加密处理过程的密钥，多个数据处理设备中的每一个设备均根据主密钥和经历加密处理过程的设备或数据的标识数据生成执行加密处理所必需的共用个别密钥。

再有，依照本发明的数据处理系统的另一个实施例，用提供内容数据的内容数据提供设备和使用内容数据的内容数据使用设备来配置成上述多个数据处理设备，内容数据提供设备和内容数据使用设备具有发布密钥生成主密钥，以生成内容数据发布密钥，它用于对内容数据提供设备与内容数据使用设备之间的流通内容数据作加密处理，所述内容数据提供设备根据发布密钥生成主密钥和是所提供的内容数据的标识符的内容标识符生成内容数据发布密钥并对内容数据执行加密处理，所述内容数据使用设备根据发布密钥生成主密钥和是所提供的

内容数据的标识符的内容标识符生成内容数据发布密钥并对内容数据执行解密处理。

再有，依照本发明的数据处理系统的另一个实施例，所述内容数据提供设备具有多个不同的发布密钥生成主密钥以生成多个不同的内容数据发布密钥、根据前述多个发布密钥生成主密钥和内容标识符生成多个不同的内容数据发布密钥、用所生成的多个发布密钥执行加密处理并生成多种类型的加密内容数据，所述内容数据使用设备具有前述内容数据提供设备所拥有的多个不同发布密钥生成主密钥中的至少一个发布密钥生成主密钥并通过用作为特有设备所拥有的发布密钥生成主密钥的同一发布密钥生成主密钥生成的发布密钥仅使加密内容数据成为可解码的。

此外，依照本发明的数据处理系统的另一个实施例，所述多个数据处理设备的每个设备均存储有同样的内容密钥生成主密钥以生成提供给内容数据加密处理过程的内容密钥，是所述多个数据处理设备之一的数据处理设备 A 将通过根据内容密钥生成主密钥和数据处理设备 A 的设备标识符生成的内容密钥而加密的内容数据存储在存储介质内，不同的数据处理设备 B 根据同一内容密钥生成主密钥和数据处理设备 A 的设备标识符生成内容密钥并根据所生成的上述内容密钥对由上述数据处理设备 A 存储在存储介质的加密内容数据作解密处理。

再有，依照本发明的数据处理系统的另一个实施例，所述多个数据处理设备是由主设备和受该主设备进行鉴别处理的从设备配置而成的，主设备和从设备均具有鉴别密钥生成主密钥，它用于在主设备与从设备之间进行鉴别处理，所述从设备根据鉴别密钥生成主密钥和是从设备的标识符的从设备标识符生成鉴别密钥并存储在从设备的存储器内，所述主设备根据鉴别密钥生成主密钥和是从设备的标识符的从设备标识符生成鉴别密钥并执行鉴别处理。

此外，本发明的第九个方面是一种数据处理方法，它执行数据加密、数据解密、数据验证、鉴别处理和签名处理中至少一个的加密处理过程，所述方法包括：密钥生成步骤，它根据生成用于加密处理的密钥的主密钥和经历加密处理的设备或数据的标识数据生成执行加密处理所必需的共用个别密钥；以及，加密处理步骤，它根据在上述密钥生成步骤中生成设备密钥执行加密处理。

再有，依照本发明的数据处理方法的另一个实施例，所述数据处理方法所执行的数据处理是对通过存储介质或通信介质的传送数据进行加密处理，所述密钥生成步骤是发布密钥生成步骤，它根据发布密钥生成主密钥 Mkdis 和是传送数据标识数据的数据标识符执行加密处理，所述主密钥 Mkdis 用于生成供对传送数据作加密处理使用的发布密钥 Kdis，所述加密处理步骤是这样的步骤，它根据在发布密钥生成步骤中生成的发布密钥 Kdis 对传送数据执行加密处理。

再有，依照本发明的数据处理方法的另一个实施例，所述数据处理方法所执行的数据处理是对向/从其传送数据的在外部连接的设备作鉴别处理，所述密钥生成步骤是鉴别密钥生成步骤，它根据用于生成外部连接的设备的鉴别密钥 Kake 的鉴别密钥生成主密钥 Mkake 和是外部连接的设备的标识数据的外部连接设备的标识符执行加密处理并生成外部连接的设备的鉴别密钥 Kake，所述加密处理步骤是这样的步骤，它根据在上述鉴别密钥生成步骤中生成的鉴别密钥 Kake 执行对外部连接的设备的鉴别处理。

再有，依照本发明的数据处理方法的另一个实施例，所述数据处理设备执行的数据处理过程是对数据的签名处理过程，所述密钥生成步骤是签名密钥生成步骤，它根据用于生成数据处理设备的数据处理设备签名密钥 Kdev 的签名密钥生成主密钥 Mkdev 以及是数据处理设备的标识数据的数据处理设备的标识符执行加密处理并生成数据处理设备的数据处理设备签名密钥 kdev，所述加密处理步骤是这样的步骤，它根据在上述鉴别密钥生成步骤中生成的鉴别密钥 Kdev 对数据执行签名处理。

再有，依照本发明的数据处理方法的另一个实施例，所述密钥生成步骤是加密处理，它将经历加密处理的设备或数据的标识数据的至少一部分用作消息并将主密钥用作加密密钥。

再有，依照本发明的数据处理方法的另一个实施例，所述加密处理过程是用 DES 算法的加密处理过程。

此外，本发明的另一个实施例是数据处理系统中的数据处理方法，所述数据处理系统包括提供内容数据的内容数据提供设备和使用内容数据的内容数据使用设备，所述方法的特征在于，所述内容数据提供设备根据发布密钥生成主密钥和是所提供的内容数据的标识符的

内容标识符生成内容数据发布密钥并对内容数据执行加密处理，所述发布密钥生成主密钥用于生成供对内容数据作加密处理使用的内容数据发布密钥，所述内容数据使用设备根据发布密钥生成主密钥和是所提供的内容数据的标识符的内容标识符生成内容数据发布密钥并对内容数据执行解密处理。

依照本发明的数据处理方法的又一个方面，所述内容数据提供设备具有多个不同的发布密钥生成主密钥以生成多个不同的内容数据发布密钥、根据前述多个发布密钥生成主密钥和内容标识符生成多个不同的内容数据发布密钥、用所生成的多个发布密钥执行加密处理并生成多种类型的加密内容数据，所述内容数据使用设备具有前述内容数据提供设备所拥有的多个不同发布密钥生成主密钥中的至少一个发布密钥生成主密钥并通过用作为特有设备所拥有的发布密钥生成主密钥的同一发布密钥生成主密钥生成的发布密钥仅对加密内容数据解密。

再有，本发明的第十一个方面是数据处理系统中的数据处理方法，该方法包括下列步骤：通过是所述多个数据处理设备之一的数据处理设备 A 将用根据内容密钥生成主密钥和数据处理设备 A 的设备标识符生成的内容密钥来加密的内容数据存储在存储介质内，所述内容密钥生成主密钥用于生成供对内容数据作加密处理使用的内容密钥；通过不同的数据处理设备 B 根据与数据处理设备 A 相同的内容密钥生成主密钥和数据处理设备 A 的设备标识符生成与所述内容密钥相同的内容密钥；以及，用数据处理设备 B 所生成的内容密钥对存储在存储介质的加密内容数据作解密处理。

本发明的第十二个方面是数据处理系统中的数据处理方法，所述数据处理系统包括主设备和受该主设备进行鉴别处理的从设备，所述方法的特征在于，所述从设备根据鉴别密钥生成主密钥和是从设备的标识符的从设备标识符生成鉴别密钥并将所生成的鉴别密钥存储在从设备的存储器内，所述鉴别密钥生成主密钥用于生成鉴别密钥，它用于在主设备与从设备之间进行鉴别处理，所述主设备根据鉴别密钥生成主密钥和是从设备的标识符的从设备标识符生成鉴别密钥并执行鉴别处理。

本发明的第十三个方面是一种程序提供介质，它提供计算机程序，以便在计算机系统上执行数据加密、数据解密、数据验证、鉴别

处理和签名处理中至少一个的加密处理过程，所述计算机程序包括：密钥生成步骤，它根据生成用于加密处理的密钥的主密钥和经历加密处理的设备或数据的标识数据生成执行加密处理所必需的共用个别密钥；以及，加密处理步骤，它根据在上述密钥生成步骤中生成设备密钥执行加密处理。

本发明的第十四个方面是一种数据处理设备，它对提供自存储介质或通信介质的内容数据进行处理，所述数据处理设备的特征在于，该设备包括：存储部，它存储数据处理设备标识符；列表验证部，它抽取包括在内容数据中的非法设备列表并执行所述列表条目与存储在存储部中的数据处理设备标识符；以及，控制部，它在所述比较处理部中的比较处理的结果表现出非法设备列表包括与数据处理标识相匹配的信息时停止执行再现内容数据或存储在记录设备的处理的至少一种处理。

依照本发明数据处理设备的另一个实施例，所述列表验证部包括一加密处理部，它对内容数据进行加密处理，所述加密处理部根据包括在内容数据中的非法设备列表的检查值来验证非法设备列表中存在或不存在篡改并仅在所述验证表明没有篡改时执行比较处理。

此外，本发明数据处理设备的又一个实施例包括非法设备列表检查值生成密钥，其特征在于，所述加密处理部执行加密处理，以便将非法设备列表检查值生成密钥应用于要加以验证的非法设备列表结构数据、生成非法设备列表检查值、执行非法设备列表检查值与包括在内容数据中的非法设备列表检查值之间的比较，从而验证在非法设备列表中存在或不存在篡改。

再有，依照本发明数据处理设备的又一个实施例，所述列表验证部包括加密处理部，它对内容数据进行加密处理，所述加密处理部执行对包括在内容数据中的加密了的非法设备列表的解密处理，并执行对源于上述解密处理的非法设备列表的比较处理。

此外，依照本发明数据处理设备的又一个实施例，所述列表验证部包括加密处理部，它对向/自其传送内容数据的记录设备进行相互鉴别处理，所述加密处理部抽取包括在内容数据中的加密了的非法设备列表，并在通过所述加密处理部所执行的相互鉴别处理而形成了对记录设备的鉴别的情况下执行与存储在存储部中的数据处理设备标识符

的比较

本发明第十五个方面是一种数据处理方法，它对提供自存储介质或通信介质的内容数据进行处理，所述方法包括：列表抽取步骤，它抽取包括在内容数据中的非法设备列表；比较处理步骤，它执行包括在列表抽取步骤中抽取出来的列表内的条目与存储在数据处理设备中存储部内的数据处理设备标识之间的比较；以及，这样的步骤，它在所述比较处理部中的比较处理的结果表现出非法设备列表包括与数据处理标识相匹配的信息时停止执行再现内容数据或存储在记录设备的处理的至少一种处理。

再有，依照本发明数据处理方法的另一个实施例，该数据处理方法还包括验证步骤，它根据包括在内容数据中的非法设备列表的检查值来验证非法设备列表中存在或不存在篡改，并且，所述比较处理步骤仅在所述验证步骤表明没有篡改时执行比较处理。

另外，依照本发明数据处理方法的又一个实施例，所述验证步骤包括以下步骤：执行加密处理，以便将非法设备列表检查值生成密钥应用于要加以验证的非法设备列表结构数据；以及，执行非法设备列表检查值与包括在内容数据中的非法设备列表检查值之间的比较，从而验证在非法设备列表中存在或不存在篡改。

另外，依照本发明数据处理方法的又一个实施例，所述方法还包括解密步骤，它对包括在内容数据中的加密了的非法设备列表作解密处理，并且，所述比较处理步骤执行对源于上述解密处理的非法设备列表作比较处理。

另外，依照本发明数据处理方法的又一个实施例，该方法还包括相互鉴别处理步骤，它对向/自其传送内容数据的记录设备进行相互鉴别处理，并且，所述比较处理步骤在通过所述加密处理步骤所执行的相互鉴别处理而形成了对记录设备的鉴别的情况下执行比较处理。

本发明的第十六个方面是一种内容数据生成方法，该方法将提供自存储介质或通信介质的内容数据生成给多个记录器/再现器，所述方法的特征在于，其组成数据包括记录器/再现器的标识符的非法设备列表被存储为内容数据的头标信息，所述非法设备列表会被排斥在使用内容数据之外。

再有，依照本发明内容数据生成方法的另一个方面，用于对非法

设备列表进行篡改检查的非法设备列表检查值也被存储为内容数据的头标信息。

再有，依照本发明内容数据生成方法的又一个方面，所述非法设备列表是加密的并存储在内容数据的头标信息中。

此外，本发明的第十七个方面是一种程序提供介质，它提供计算机程序，此程序使计算机系统执行对提供自存储介质或通信介质的内容数据的处理，其特征在于，所述计算机程序包括：列表抽取步骤，它抽取包括在内容数据中的非法设备列表；比较处理步骤，它执行包括在列表抽取步骤中抽出的列表内的条目与存储在数据处理设备中的存储部内的数据处理设备标识符之间的比较；以及，这样的步骤，它在所述比较处理部中的比较处理的结果表现出非法设备列表包括与数据处理标识相匹配的信息时停止执行再现内容数据或存储在记录设备的处理的至少一种处理。

本发明的第十八个方面是一种对通过记录或通信介质提供的内容数据进行处理的数据处理设备，所述设备包括：加密处理部，它对内容数据进行加密处理；控制部，它用于对加密处理部进行控制；系统共用密钥，它用于加密处理部中的加密处理过程，所述系统共用密钥为使用内容数据的其它数据处理设备所共用；以及，设备专用密钥或设备专用标识符中的至少一个，所述设备专用密钥为用于加密处理部中的加密处理的数据处理设备所专用，所述设备专用标识符用于生成上述设备专用密钥，所述数据处理设备的特征在于，前述加密处理部配置成：根据内容数据的使用模式通过应用系统共用密钥或设备专用密钥中的一个执行加密处理。

再有，在本发明的数据处理设备的另一个实施例中，所述加密处理部根据包括在内容数据中的使用限制信息通过应用系统共用密钥或设备专用密钥中的一个执行加密处理。

还有，本发明的数据处理设备的又一个实施例包括用于记录内容数据的记录设备，所述数据处理设备的特征在于，上述加密处理部在被施加以内容数据应仅用于上述特有数据处理设备的使用限制时通过用用于内容数据的设备专用密钥执行加密处理而生成要存储在记录设备中的数据，并且，在所述内容数据也可用于除特有数据处理设备以外的设备的情况下通过用系统共用密钥对内容数据进行加密处理而生

成要存储在记录设备中的数据。

再有，本发明的数据处理设备的再一个实施例包括为数据处理设备所专用的签名密钥Kdev和为多个数据处理设备所共用的系统签名密钥 Keys，所述数据处理设备的特征在于，上述加密处理部在前述内容数据存储在被施加以内容数据应仅用于上述特有数据处理设备的记录设备中时通过将设备专用签名密钥kdev应用于内容数据的加密处理而生成设备专用检查值，并在所述内容数据存储在带有也可用于除特有数据处理设备以外的设备的记录设备中时通过将系统签名密钥keys应用于内容数据的加密处理而生成总体检查值，而且，所述控制部控制将加密处理部所生成的设备专用检查值或总体检查值中的一个连同内容数据存储在记录设备内。

再有，本发明的数据处理设备的再一个实施例包括为数据处理设备所专用的签名密钥Kdev和为多个数据处理设备所共用的系统签名密钥 Keys，所述数据处理设备的特征在于，上述加密处理部在被施加以内容数据应仅用于上述特有数据处理设备使用限制时生成设备专用检查值以便将设备专用签名密钥Kdev应用于内容数据并对所生成的设备专用检查值执行比较处理，而且在再现也可用于除特有数据处理设备以外的设备的内容数据时通过将系统签名密钥keys应用于内容数据的加密处理而生成总体检查值，还对所生成的总体检查值进行比较处理，并且，仅在形成了与设备专用检查值的比较或在形成与总体检查值的比较时，所述控制部通过由加密处理部来继续对内容数据进行处理而生成可再现的解密数据。

再有，本发明的数据处理设备的又一个实施例包括记录数据处理设备签名密钥主密钥Mkdev和数据处理设备标识符 IDdev，所述数据处理设备的特征在于，前述加密处理部根据记录数据处理设备签名密钥主密钥 Mkdev 和数据处理设备标识符 IDdev 通过加密处理过程生成用作数据处理设备专用于密钥的签名密钥Kdev。

此外，在本发明的数据处理设备的又一个实施例中，所述加密处理部通过将记录数据处理设备签名密钥主密钥 Mkdev 应用于数据处理设备标识符 IDdev 的DES加密处理而生成签名密钥Kdev。

再有，在本发明的数据处理设备的又一个实施例中，所述加密处理部通过对内容数据执行加密处理而生成中间整体性检查值并执行将

数据处理设备专用密钥或系统共用密钥应用到中间整体性检查值的加密处理。

再有，在本发明的数据处理设备的还一个实施例中，所述加密处理部通过对包含至少一个因将内容数据分成多个部分获得的部分数据项目的部分数据集进行加密处理而生成部分整体性检查值并通过对包含所生成的部分整体性检查值的部分整体性检查值集数据串进行加密处理而生成中间整体性检查值。

本发明的第十九个方面是一种数据处理方法，它对通过记录介质或通信介质提供的内容数据进行处理，所述方法的特征在于，根据内容数据的利用模式选定为使用内容数据的其它数据处理设备所共用的加密处理系统共用密钥或为数据处理设备所专用的设备专用密钥中的一个，并且，通过将选定的加密处理密钥应用于内容数据而执行加密处理。

再有，本发明数据处理方法的另一个实施例的特征在于，所述加密处理密钥选择步骤是这样的步骤：根据包含在内容数据中的使用限制信息进行选择。

此外，本发明数据处理方法的又一个实施例的特征在于，所述将内容数据存储记录设备内的处理过程在被施加以内容数据应仅用于上述特有数据处理设备的使用限制时通过执行将设备专用密钥应用于内容数据的加密处理而生成要存储在记录设备中的数据，并且，在所述内容数据也可用于除特有数据处理设备以外的设备的情况下通过用系统共用密钥对内容数据进行加密处理而生成要存储在记录设备中的数据。

再有，本发明数据处理方法的又一个实施例的特征在于，在前述内容数据存储在被施加以内容数据应仅用于上述特有数据处理设备的记录设备中时，将内容数据记录到记录设备的处理过程会通过将设备专用签名密钥 kdev 应用于内容数据的加密处理而生成设备专用检查值，并在所述内容数据存储在带有也可用于除特有数据处理设备以外的设备的记录设备中时通过将系统签名密钥keys应用于内容数据的加密处理而生成总体检查值，而且，将所生成的设备专用检查值或总体检查值中的一个连同内容数据存储在记录设备内。

再有，本发明的数据处理方法的再一个实施例的特征在于，在再

现被施加以内容数据应仅用于上述特有数据处理设备的使用限制的内容数据时，所述内容数据再现处理过程通过将设备专用签名密钥 Kdev 应用于内容数据的加密处理而生成设备专用检查值并对所生成的设备专用检查值执行比较处理，而且在再现也可用于除特有数据处理设备以外的设备的内容数据时通过将系统签名密钥 keys 应用于内容数据的加密处理而生成总体检查值，还对所生成的总体检查值进行比较处理，并且，仅在形成了与设备专用检查值的比较或在形成与总体检查值的比较时，再现的内容数据。

再有，本发明的数据处理方法的还一个实施例还包括下列步骤：根据数据处理设备签名密钥主密钥 Mkdev 和数据处理设备标识符 IDdev 通过加密处理过程生成用作数据处理设备专用于密钥的签名密钥 Kdev。

此外，在本发明的数据处理方法的又一个实施例的特征在于，所述签名密钥 Kdev 生成步骤是这样的步骤：通过将数据处理设备签名密钥主密钥 Mkdev 应用于数据处理设备标识符 IDdev 的 DES 加密处理而生成签名密钥 Kdev。

再有，在本发明的数据处理方法还包括这样的步骤：通过对内容数据执行加密处理而生成中间整体性检查值，所述方法的特征在于，执行将数据处理设备专用密钥或系统共用密钥应用到中间整体性检查值的加密处理。

再有，在本发明的数据处理方法的还一个实施例的特征在于，该方法还通过对包含至少一个因将内容数据分成多个部分获得的部分数据项目的部分数据集进行加密处理而生成部分整体性检查值并通过对包含所生成的部分整体性检查值的部分整体性检查值集数据串进行加密处理而生成中间整体性检查值。

本发明的第二十个方面是一种提供计算机程序的程序提供介质，所述程序使计算机系统执行对通过存储介质或通信介质提供的内容数据的数据处理，所述计算机程序包括这样的步骤：根据内容数据的利用模式选定为使用内容数据的其它数据处理设备所共用的加密处理系统共用密钥或为数据处理设备所专用的设备专用密钥中的一个，并且，执行将选定的加密处理密钥应用于内容数据的加密处理。

本发明的第二十一个方面是一种对通过记录或通信介质提供的内

容数据进行处理的数据处理设备，所述设备包括：加密处理部，它对内容数据进行加密处理；控制部，它用于对加密处理部进行控制；所述数据处理部的特征在于，上述加密处理部配置成：生成要加以验证的包括在数据中的内容块数据单元中的内容检查值、执行对所生成的内容检查值的比较，从而执行对数据中各内容块数据的有效性的验证处理。

本发明数据处理设备的又一个实施例包括内容检查值生成密钥并且特征在于，所述加密处理部根据要加以验证的内容块生成内容中间值并通过执行将内容检查值生成密钥应用于内容中间值的加密处理过程而生成内容检查值。

再有，本发明数据处理设备的又一个实施例的特征在于，在对要加以验证的内容块数据进行加密时，所述加密处理部通过对整个的解密信息执行预定的操作处理而生成内容中间值，所述解密信息是通过对预定数量字节单元中的内容块数据作解密处理而获得的，并且，在不对要加以验证的内容块数据进行加密时，所述加密处理部通过对预定数量字节单元中的整个内容块数据执行预定的操作处理而生成内容中间值。

另外，本发明数据处理设备的还一个实施例的特征在于，所述加密处理部所进行的应用于中间整体性检查值生成处理过程的预定操作处理是异或操作。

再有，本发明数据处理设备的还一个实施例的特征在于，所述加密处理部具有 CBC 模式的加密处理结构以及在要加以验证的内容块数据是 CBC 模式的解密处理时的应用于内容中间值生成处理过程的解密处理过程。

再有，本发明数据处理设备的另一个实施例的特征在于，所述加密处理部的 CBC 模式下的加密处理是这样的结构，其中，共用密钥加密处理过程仅多次应用于要加以处理的消息串的一部分。

再有，本发明数据处理设备的又一个实施例的特征在于，当内容块数据包含多个部分且包括在内容数据块中的某些部分要加以验证时，所述加密处理部就根据要加以验证的部分生成内容检查值、执行对所生成的内容检查值的比较处理，从而对数据中内容块数据单元中的有效性执行验证处理。

再有，本发明数据处理设备的另一个实施例的特征在于，当内容块数据包含多个部分且有一部分要加以验证时，所述加密处理部就通过执行加密处理生成数据检查值，所述加密处理将内容检查值生成密钥应用于这样的值，该值是通过在预定数量字节单元中对整个解密信息进行异或操作而获得的，而所述解密信息则是在对要加以验证的部分进行加密的情况下通过对要加以验证的部分进行解密处理而获得的，并且，所述加密处理部通过执行加密处理生成数据检查值，所述加密处理将内容检查值生成密钥应用于这样的值，该值是在不对要加以验证的部分进行加密的情况下通过在预定数量字节单元中对要加以验证的整个部分进行异或操作而获得的。

再有，本发明数据处理设备的还一个实施例的特征在于，当内容块数据包含多个部分且有多个部分要加以验证时，所述加密处理部作为内容检查值使用通过执行加密处理所获得的结果，所述加密处理将内容检查值生成密钥应用于通过执行将内容检查值生成密钥用于各部分的加密处理而获得的部分检查值的链接数据。

再有，本发明数据处理设备的又一个实施例的特征在于，所述加密处理部还包括记录设备，它用于存储包含有效性已得到验证的内容块数据的内容数据。

另外，本发明数据处理设备的又一个实施例的特征在于，当在比较处理过程中未对加密处理部中的内容检查值形成比较时，所述控制部就停止存储到记录设备内。

再有，本发明数据处理设备的又一个实施例的特征在于，所述加密处理部还包括再现处理部，它用于再现有效性已被验证了的数据。

再有，本发明数据处理设备的另一个实施例的特征在于，当在比较处理过程中未对加密处理部中的内容检查值形成比较时，所述控制部就停止再现处理部中的再现处理。

本发明的第二十二个方面是一种对通过记录介质或通信介质提供的内容数据进行处理的数据处理方法，其特征在于，生成包括在数据内的要加以验证的内容块数据单元中整体性检查值内容检查值、执行对所生成的内容检查值的比较，从而执行数据中内容块数据单元内的有效性的验证处理。

再有，本发明的数据处理方法的另一个实施例的特征在于，根据

要加以验证的内容块数据生成内容中间值并通过执行将内容检查值生成密钥应用于所生成的内容中间值的加密处理而生成内容检查值。

再有，本发明的数据处理方法的另一个实施例的特征在于，在对要加以验证的内容块数据进行加密时，通过对整个的解密信息执行预定的操作处理而生成内容中间值，所述解密信息是通过对预定数量字节单元中的内容块数据作解密处理而获得的，并且，在不对要加以验证的内容块数据进行加密时，通过对预定数量字节单元中的整个内容块数据执行预定的操作处理而生成内容中间值。

另外，本发明数据处理方法的还一个实施例的特征在于，所述应用于中间整体性检查值生成处理过程的预定操作处理是异或操作。

再有，本发明数据处理方法的还一个实施例的特征在于，在内容中间值生成处理过程中，在对要加以验证的内容块数据进行加密处理时应用于内容中间值生成处理过程的解密处理过程是 CBC 模式下的解密处理。

再有，本发明数据处理方法的另一个实施例的特征在于，在 CBC 模式下的加密处理结构中，将共用密钥加密处理过程仅多次应用于要加以处理的消息串的一部分。

再有，本发明数据处理方法的又一个实施例的特征在于，当内容块数据包含多个部分且包括在内容数据块中的某些部分要加以验证时，就根据要加以验证的部分生成内容检查值、执行对所生成的内容检查值的比较处理，从而对数据中内容块数据单元中的有效性执行验证处理。

再有，本发明数据处理方法的另一个实施例的特征在于，当内容块数据包含多个部分且有一部分要加以验证时，就通过执行加密处理生成数据检查值，所述加密处理将内容检查值生成密钥应用于这样的值，该值是通过在预定数量字节单元中对整个解密信息进行异或操作而获得的，而所述解密信息则是在对要加以验证的部分进行加密的情况下通过对要加以验证的部分进行解密处理而获得的，并且，通过执行加密处理生成数据检查值，所述加密处理将内容检查值生成密钥应用于这样的值，该值是在不对要加以验证的部分进行加密的情况下通过在预定数量字节单元中对要加以验证的整个部分进行异或操作而获得的。

再有，本发明数据处理方法的还一个实施例的特征在于，当内容块数据包含多个部分且有多个部分要加以验证时，作为内容检查值使用通过执行加密处理所获得的结果，所述加密处理将内容检查值生成密钥应用于通过执行将内容检查值生成密钥用于各部分的加密处理而获得的部分检查值的链接数据。

再有，本发明数据处理方法的又一个实施例还包括这样的步骤，它存储包含有有效性已得到验证的内容块数据的内容数据。

另外，本发明数据处理方法的又一个实施例的特征在于，当在比较处理过程中未对内容检查值形成比较时，所述控制部就停止存储到记录设备内。

此外，本发明数据处理方法的另一个实施例还包括这样的步骤，它再现有效性已得到验证的数据。

再有，本发明数据处理方法的另一个实施例的特征在于，当在比较处理过程中未对内容检查值形成比较时，就停止再现处理。

本发明的第二十三个方面是一种用于内容数据验证处理的内容数据验证值赋值方法，其特征在于，生成要加以验证的内容块数据单元的内容检查值、将所生成的内容检查值赋给包含要加以检证的内容块数据的内容数据。

再有，本发明内容数据验证值赋值方法的另一个实施例的特征在于，通过应用内容检查值生成密钥的加密处理将要加以检查的内容块数据用作消息而生成内容检查值。

还有，本发明内容数据验证值赋值方法的又一个实施例的特征在于，通过根据要加以验证的内容块数据生成内容中间值并执行将内容检查值生成密钥应用于内容中间值的加密处理而生成内容检查值。

此外，本发明内容数据验证值赋值方法的还一个实施例的特征在于，通过在 CBC 模式下对要加以验证的内容块数据进行加密处理而生成内容检查值。

还有，本发明内容数据验证值赋值方法的再一个实施例的特征在于，在 CBC 模式下的加密处理结构是这样的结构，其中，将共用密钥加密处理过程仅多次应用于要加以处理的消息串的一部分。

再有，本发明内容数据验证值赋值方法的还一个实施例的特征在于，当内容块数据包含多个部分且包括在内容数据块中的某些部分要

加以验证时，就根据要加以验证的部分生成内容检查值并将所生成的内容检查值赋给包含要加以验证的内容块数据的内容数据。

再有，本发明内容数据验证值赋值方法的还一个实施例的特征在于，当内容块数据包含多个部分且有一部分要加以验证时，就通过执行加密处理生成内容检查值，所述加密处理将内容检查值生成密钥应用于这样的值，该值是通过在预定数量字节单元中对整个解密信息进行异或操作而获得的，而所述解密信息则是在对要加以验证的部分进行加密的情况下通过对要加以验证的部分进行解密处理而获得的，并且，通过执行加密处理生成内容检查值，所述加密处理将内容检查值生成密钥应用于这样的值，该值是在不对要加以验证的部分进行加密的情况下通过在预定数量字节单元中对要加以验证的整个部分进行异或操作而获得的，以及，将所生成的内容检查值赋给包含要加以验证的内容块数据的内容数据。

再有，本发明内容数据验证值赋值方法的另一个实施例的特征在于，当内容块数据包含多个部分且有多个部分要加以验证时，作为内容检查值使用通过执行加密处理所获得的结果，所述加密处理将内容检查值生成密钥应用于通过执行将内容检查值生成密钥用于各部分的加密处理而获得的部分检查值的链接数据，以及，将所生成的内容检查值赋给包含要加以验证的内容块数据的内容数据。

本发明的第二十四个方面是一种程序提供介质，它提供计算机程序以便对通过记录介质或通信介质提供的内容数据进行数据处理，所述计算机程序包括下列步骤：生成包括在数据内的要加以验证的内容块数据单元中的内容检查值、执行对所生成的内容检查值的比较，从而执行数据中内容块数据单元内的有效性的验证处理。

本发明的第二十五个方面是一种数据处理设备，它用于执行这样的处理过程，该处理过程就内容数据的记录设备生成存储数据，所述内容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的信息，所述数据处理设备的特征在于，在作为记录设备中存储对象的内容数据是由存储在头标部内的是加密密钥数据 Kdis[Kcon]的数据构成的情况下，上述数据处理设备具有这样的结构，它用于执行从头标部中提取加密密钥数据 Kdis[Kcon]的处理并执行解密处理以生成解密数据 Kcon、生成通过加

密密钥 Kstr 应用于加密处理过程的新加密密钥数据 Kstr[Kcon]并将该新加密密钥数据 Kstr[Kcon]存储进内容数据的头标部、以及将不同的加密密钥 Kstr 应用于所生成的解密数据 Kcon 以执行加密处理，上述加密密钥数据 Kdis[Kcon]是通过加密密钥 Kdis 应用于加密处理的内容块的加密密钥 Kcon，

本发明的第二十六个方面是一种数据处理设备，它用于执行这样的处理过程，该处理过程就内容数据的记录设备生成存储数据，所述内容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的信息，所述数据处理设备的特征在于，在包括在作为记录设备存储对象的内容数据中的数据块是由用加密密钥 Kblc 来加密的内容以及用加密密钥 Kcon 来加密的加密密钥数据 Kcon[Kblc]构成的并且具有将是通过加密密钥 Kdis 应用于加密处理的加密密钥 Kcon 的加密密钥数据 Kdis[Kcon]存储在头标部中的结构的情况下，上述数据处理设备具有这样的结构，它用于执行从头标部中提取加密密钥数据 Kdis[Kcon]的处理并执行解密处理以生成解密数据 Kcon、生成是通过加密密钥 Kstr 应用于加密处理过程的加密密钥数据 Kstr[Kcon]并将该加密密钥数据 Kstr[Kcon]存储进内容数据的头标部、以及将不同的加密密钥 Kstr 应用于所生成的解密数据 Kcon 以执行加密处理。

再有，本发明的第二十七个方面是这样一种数据处理设备，它用于执行这样的处理过程，该处理过程就内容数据的记录设备生成存储数据，所述内容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的信息，所述数据处理设备的特征在于，在包括在作为记录设备存储对象的内容数据中的数据块是由用加密密钥 Kblc 来加密的内容以及用加密密钥 Kdis 来加密的加密密钥数据 Kdis[Kblc]构成的情况下，上述数据处理设备具有这样的结构，它用于执行从头标部中提取加密密钥数据 Kdis[Kblc]的处理并执行解密处理以生成解密数据 Kblc、生成通过加密密钥 Kstr 应用于加密处理过程的加密密钥数据 Kstr[Kblc]并将该加密密钥数据 Kstr[Kblc]存储进内容数据的头标部、以及将不同的加密密钥 Kstr 应用于所生成的解密数据 Kblc 以执行加密处理。

此外，本发明的第二十八个方面是一种用于生成内容数据的内容

数据生成方法，该方法包括：将多个由包括声音信息、图像信息和程序数据中至少任一种在内的数据构成的内容块连接起来；通过加密密钥 Kcon 将加密处理过程应用于包括在上述多个内容块中的内容块的至少一部分；生成加密密钥数据 kdis[Kcon] 并将加密密钥 Kdis 存储在内容数据的头标部内，所述加密密钥数据 kdis[Kcon] 是应用于加密密钥 Kdis 所进行的加密处理过程的加密密钥 Kcon；以及，生成包括多个内容块和头标部的内容数据。

再有，本发明内容数据生成方法的一个实施例的特征在于，该方法还包括这样的处理过程：生成块信息，该信息包括内容数据的标识信息、内容数据的数据长度、包括内容数据的数据类型、内容块的数据长度和加密处理过程存在与否在内的使用策略信息；以及，将块信息存储到头标部内。

再有，本发明内容数据生成方法的一个实施例的特征在于，该内容数据生成方法包括：根据包括头标部在内的信息的一部分生成部分检查值并将该部分检查值存储到头标部内的处理过程；以及，根据上述部分检查值生成总检查值并将该总检查值存储到头标部内。

还有，本发明内容数据生成方法的一个实施例的特征在于，所述部分检查值的生成处理过程和总检查值的生成处理过程在将是检查对象的数据用作消息并将检查值生成密钥用作加密密钥的情况下应用并执行 DES 加密处理算法。

此外，本发明内容数据生成方法的一个实施例的特征在于，该内容数据生成方法还通过加密密钥 Kbit 将加密处理用于块信息并将是用加密密钥 Kdis 生成的加密密钥 Kbit 的加密密钥数据 kdis[Kbit] 存储进头标部。

另外，本发明内容数据生成方法的一个实施例的特征在于，所述内容块中的多个块内的各个块被生成为共用固定数据长度。

还有，本发明内容数据生成方法的一个实施例的特征在于，按其中加密数据部和非加密数据部规则排列的结构生成所述内容块中的多个块内的各个块。

本发明的第二十九个方面是用于生成内容数据的内容数据生成方法，该方法包括：将多个包括声音信息、图像信息和程序数据中至少任一种在内的内容块连接起来；用加密数据部和一组加密密钥数据

Kcon[Kblc]构成所述多个内容块的至少一部分，所述加密数据部是按加密密钥 Kblc 包括声音信息、图像信息和程序数据中至少任一种在内的数据，而所述加密密钥数据 Kcon[Kblc]则是应用于加密密钥 kcon 所进行的加密处理过程的加密数据部的加密密钥 Kblc；生成加密密钥数据 kdis[Kcon]并将所生成检查值加密密钥数据 kdis[Kcon]存储在内容数据的头标内，所述加密密钥数据 kdis[Kcon]是应用于加密密钥 Kdis 所进行的加密处理过程的加密密钥 Kcon；以及，生成包括多个内容块和头标部的内容数据。

本发明的第三十个方面是用于生成内容数据的内容数据生成方法，该方法包括：将多个包括声音信息、图像信息和程序数据中至少任一种在内的内容块连接起来；用加密数据部和一组加密密钥数据 Kdis[Kblc]构成所述多个内容块的至少一部分，所述加密数据部是按加密密钥 Kblc 包括声音信息、图像信息和程序数据中至少任一种在内的数据，而所述加密密钥数据 Kdis[Kblc]则是应用于加密密钥 kdis 所进行的加密处理过程的加密数据部的加密密钥 Kblc；以及，生成包括多个内容块和头标部的内容数据。

本发明的第三十一个方面是一种数据处理方法，它用于执行这样的处理过程，该处理过程用于将内容数据存储在记录设备内，所述内容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的信息，所述方法包括：在作为记录设备存储对象的内容数据是由存储在头标部中数据构成的情况下，从头标部中提取加密密钥数据 Kdis[Kcon] 并执行解密处理以生成解密数据 Kcon，所述存储在头标部中数据是加密密钥数据 Kdis[Kcon]，该加密密钥数据 Kdis[Kcon]是通过加密密钥 Kdis 应用于加密处理器的内容块的加密密钥 Kcon；通过将不同的加密密钥 Kstr 应用于所生成的解密数据 Kcon 以执行解密处理而生成新的加密密钥数据 Kstr[Kcon]，该新加密密钥数据 Kstr[Kcon]可通过加密密钥 Kstr 应用于加密处理过程；以及，将所生成的加密密钥数据 Kstr[KconJ 存储进内容数据的头标部内并将所述头标部连同所述多个内容块存储进记录设备。

本发明的第三十二个方面是一种数据处理方法，它用于执行这样的处理过程，该处理过程用于将内容数据存储在记录设备内，所述内

容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的信息，所述方法包括：在包括在作为记录设备存储对象的内容数据中的数据块是由用加密密钥 Kblc 来加密的内容以及用加密密钥Kcon来加密的加密密钥数据Kcon[Kblc]构成的并且具有将是通过加密密钥 Kdis 应用于加密处理的加密密钥 Kcon 的加密密钥数据 Kdis[Kcon]存储在头标部中的结构的情况下，从头标部中提取加密密钥数据 Kdis[Kcon]并执行解密处理以生成解密数据 Kcon；通过将不同的加密密钥 Kstr 应用于所生成的解密数据 Kcon 以执行解密处理而生成是通过加密密钥Kstr应用于加密处理过程的加密密钥数据 Kstr[Kcon]；以及，将所生成的加密密钥数据 Kstr[Kcon]存储进内容数据的头标部并将所述头标部连同所述多个内容块存储进记录设备。

再有，本发明的第三十三个方面是这样一种数据处理方法，它用于执行这样的处理过程，该处理过程将内容数据存储在记录设备内，所述内容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的信息，所述方法包括：在包括在作为记录设备存储对象的内容数据中的数据块是由用加密密钥 Kblc 来加密的内容以及用加密密钥 Kdis 来加密的加密密钥数据 Kdis[Kblc]构成的情况下，从头标部中提取加密密钥数据 Kdis[Kblc]并执行对加密密钥Kblc的解密处理以生成解密数据Kblc;通过将不同的加密密钥 Kstr 应用于所生成的解密数据 Kblc 以执行解密处理而生成通过加密密钥 Kstr 应用于加密处理过程的加密密钥数据 Kstr[Kblc]；以及将所生成的加密密钥数据 Kstr[Kblc]存储进内容数据的头标部并将所述头标部连同所述多个内容块存储进记录设备。

本发明的第三十四个方面是一种用于提供计算机程序的程序提供介质，所述计算机程序能执行生成处理过程：将数据存储至在内容数据的记录设备内，所述内容数据具有：多个内容块，其中，对至少一部分数据块进行加密；以及，头标部，它存储有与内容块有关的要在计算机系统上执行的信息，程序提供介质的特征在于，上述计算机程序包括：在作为记录设备中存储对象的内容数据是由存储在头标部内的是加密密钥数据 Kdis[Kcon]的数据构成的情况下，从头标部中提取加密密钥数据 Kdis[Kcon]并执行解密处理以生成解密数据 Kcon；通过

将不同的加密密钥 Kstr 应用于所生成的解密数据 Kcon 以执行解密处理而生成通过加密密钥 Kstr 应用于加密处理过程的新加密密钥数据 Kstr[Kcon]；以及，将所生成的加密密钥数据 Kstr[Kcon]存储进内容数据的头标部，而所述加密密钥数据 Kdis[Kcon]是通过加密密钥 Kdis 应用于加密处理的内容块的加密密钥 Kcon。

本发明的第三十五个方面是一种数据处理设备，它用于对存储介质或通信介质提供的内容数据进行再现处理，所述数据处理设备的特征在于，该设备包括：内容数据分析部，它用于执行对包括压缩内容和压缩内容的扩展处理程序在内的内容数据的内容数据分析并执行从内容数据中对压缩内容和扩展处理程序的抽取处理；扩展处理部，它用于用包括在因内容数据分析部的分析而获得的内容数据中的扩展处理程序来执行对包括在内容数据中的内容数据的扩展处理。

再有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，该设备还包括：数据存储部，它用于存储压缩的内容，这些内容是由前述数据分析部所抽取的；以及，程序存储部，它用于存储由前述内容数据分析部抽取的扩展处理程序，并且，所述设备的特征在于，前述扩展处理部具有这样的结构，它用于通过将存储在程序存储部内的扩展处理程序应用于压缩内容而对存储在数据存储部内的压缩内容进行扩展处理。

此外，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，前述内容数据分析部具有这样的结构，它用于根据包括在内容数据中的头标信息获得内容数据的结构信息并对内容数据进行分析。

再有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，压缩内容的再现优先权信息包括在头标信息内，如果存在有多个是扩展处理部的扩展处理过程的对象的压缩内容，则扩展处理部具有这样的结构，它用于根据在内容数据分析部中获得的头标信息内的优先权信息按优先权顺序地执行内容扩展处理。

还有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，该设备包括：显示装置，它用于显示是扩展处理的对象的压缩内容的信息；以及，输入装置，它用于输入从显示在显示装置上的内容信息中选出的再现内容标识数据，并且，所述设备的特征

在于，扩展处理部具有这样的结构，它根据输入自输入装置的再现内容标识数据对与所述标识数据相对应的压缩内容执行扩展处理。

另外，本发明的第三十六个方面是一种数据处理设备，它用于对存储介质或通信介质提供的内容数据进行再现处理，所述数据处理设备的特征在于，该设备包括：内容数据分析部，它用于接收包括压缩内容或扩展处理程序在内的内容数据，以便根据包括在接收到的内容数据中的头标信息辨别出内容数据是具有压缩内容还是具有扩展处理程序，同时，如果内容数据具有压缩内容，就根据内容数据的头标信息获得一种类型的应用于压缩内容的压缩处理程序，如果内容数据具有扩展处理程序，则根据内容数据的头标信息获得一种类型的扩展处理程序；扩展处理部，它用于执行对压缩内容的扩展处理，所述设备的特征在于，前述扩展处理部具有这样的结构，它用于根据内容数据分析部所分析的扩展处理程序的类型选择适用于内容数据分析部分析的压缩内容的压缩处理程序的类型的扩展处理程序，并用选定的扩展处理程序执行扩展处理。

再有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，该设备还包括：数据存储部，它用于存储压缩的内容，这些内容是由前述数据分析部所抽取的；以及，程序存储部，它用于存储由前述内容数据分析部抽取的扩展处理程序，并且，所述设备的特征在于，前述扩展处理部具有这样的结构，它用于通过将存储在程序存储部内的扩展处理程序应用于压缩内容而对存储在数据存储部内的压缩内容进行扩展处理。

再有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，压缩内容的再现优先权信息包括在头标信息内，如果存在有多个是扩展处理过程的对象的压缩内容，则扩展处理部中的内容扩展处理具有这样的结构，它用于根据在内容数据分析部中获得的头标信息内的优先权信息按优先权顺序地执行内容扩展处理。

还有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，该设备包括：检索装置，它用于检索扩展处理程序，所述设备的特征在于，上述检索装置具有这样的结构，它用于检索出适用于内容数据分析部分析的压缩内容的压缩处理程序的类型的扩展处理程序，而程序存储装置则可由数据处理设备作为检索的对象来加

以访问。

再有，在本发明数据处理设备的一个实施例中，所述数据处理设备的特征在于，该设备包括：显示装置，它用于显示是扩展处理的对象的压缩内容的信息；以及，输入装置，它用于输入从显示在显示装置上的内容信息中选出的再现内容标识数据，并且，所述设备的特征在于，扩展处理部具有这样的结构，它根据输入自输入装置的再现内容标识数据对与所述标识数据相对应的压缩内容执行扩展处理。

本发明的第三十七个方面是一种数据处理方法，它用于对存储介质或通信介质提供的内容数据进行再现处理，所述数据处理方法的特征在于，该方法包括：内容数据分析步骤，它执行对包括压缩内容和压缩内容的扩展处理程序在内的内容数据的内容数据分析并执行从内容数据中对压缩内容和扩展处理程序的抽取处理；扩展处理步骤，它用包括在因内容数据分析部的分析而获得的内容数据中的扩展处理程序来执行对包括在内容数据中的内容数据的扩展处理。

再有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，该方法还包括：数据存储步骤，它存储压缩的内容，这些内容是由前述数据分析部所抽取的；以及，程序存储步骤，它存储由前述内容数据分析部抽取的扩展处理程序，并且，所述方法的特征在于，前述扩展处理部具有这样的结构，它用于通过将在程序存储步骤内存储的扩展处理程序应用于压缩内容而对数据存储步骤内存储的压缩内容进行扩展处理。

此外，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，前述内容数据步骤根据包括在内容数据中的头标信息获得内容数据的结构信息并对内容数据进行分析。

再有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，压缩内容的再现优先权信息包括在头标信息内，如果存在有多个是扩展处理部的扩展处理过程的对象的压缩内容，则扩展处理步骤根据在内容数据分析步骤中获得的头标信息内的优先权信息按优先权顺序地执行内容扩展处理。

还有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，该方法包括：显示步骤，它将是扩展处理的对象的压缩内容的信息显示到显示装置上；以及，输入步骤，它用于输入从显

示在显示装置上的内容信息中选出的再现内容标识数据，并且，所述方法的特征在于，扩展处理步骤根据输入自输入步骤的再现内容标识数据对与所述标识数据相对应的压缩内容执行扩展处理。

另外，本发明的第三十八个方面是一种数据处理方法，它用于对存储介质或通信介质提供的内容数据的进行再现处理，所述数据处理方法的特征在于，该设备包括：内容数据分析步骤，它接收包括压缩内容或扩展处理程序在内的内容数据，以便根据包括在接收到的内容数据中的头标信息辨别出内容数据是具有压缩内容还是具有扩展处理程序，同时，如果内容数据具有压缩内容，就根据内容数据的头标信息获得一种类型的应用于压缩内容的压缩处理程序，如果内容数据具有扩展处理程序，则根据内容数据的头标信息获得一种类型的扩展处理程序；选择步骤，它根据内容数据分析步骤中所分析的扩展处理程序的类型选择适用于内容数据分析步骤中分析的压缩内容的压缩处理程序的类型的扩展处理程序；以及，扩展处理步骤，它用选择步骤中选定的扩展处理程序执行扩展处理。

再有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，该方法还包括：数据存储步骤，它存储压缩的内容，这些内容是由前述数据分析部所抽取的；以及，程序存储步骤，它用于存储由前述内容数据分析部抽取的扩展处理程序，并且，所述方法的特征在于，前述扩展处理步骤通过将在程序存储步骤内存储的扩展处理程序应用于压缩内容而对在数据存储步骤部内存储的压缩内容进行扩展处理。

再有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，压缩内容的再现优先权信息包括在头标信息内，如果存在有多个是扩展处理过程的对象的压缩内容，则扩展处理步骤根据在内容数据分析步骤中获得的头标信息内的优先权信息按优先权顺序地执行内容扩展处理。

还有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，该方法包括：检索步骤，它检索扩展处理程序，所述方法的特征在于，上述检索步骤检索出适用于内容数据分析步骤分析的压缩内容的压缩处理程序的类型的扩展处理程序，而程序存储装置则可由数据处理设备作为检索的对象来加以访问。

再有，在本发明数据处理方法的一个实施例中，所述数据处理方法的特征在于，该方法包括：显示步骤，它用于显示是扩展处理的对象的压缩内容的信息；以及，输入步骤，它输入从显示在显示装置上的内容信息中选出的再现内容标识数据，并且，所述方法的特征在于，扩展处理步骤根据输入自输入装置的再现内容标识数据对与所述标识数据相对应的压缩内容执行扩展处理。

此外，本发明的第三十九个方面是一种内容数据生成方法，该方法对提供自存储介质或通信介质的内容数据进行生成处理，所述方法的特征在于，生成内容数据，其中，压缩内容和压缩内容的扩展处理程序是组合在一起的。

再有，在本发明内容数据生成方法的一个实施例中，该内容数据生成方法的特征在于，将内容数据的结构信息增加为内容数据的头标信息。

此外，在本发明内容数据生成方法的一个实施例中，该内容数据生成方法的特征在于，将包括在内容数据中的内容的再现优先权信息作为内容数据的头标信息。

再有，本发明的第四十个方面是一种内容数据生成方法，该方法对提供自存储介质或通信介质的内容数据进行生成处理，所述方法的特征在于，生成内容数据，其中，将一种类型的用于标识内容数据具有压缩内容还是具有扩展处理程序的内容数据增加为头标信息，如果所述内容数据具有压缩内容，则将一种类型的应用于压缩内容的压缩处理程序增加为头标信息，如果内容数据具有扩展处理程序，则将一种类型的扩展处理程序增加为头标信息。

此外，在本发明内容数据生成方法的一个实施例中，该内容数据生成方法的特征在于，将包括在内容数据中的内容的再现优先权信息作为内容数据的头标信息。

此外，本发明的第四十一个方面是一种程序提供介质，它提供计算机程序，此程序使计算机系统执行对提供自存储介质或通信介质的内容数据的再现处理，其特征在于，所述计算机程序包括：内容数据分析步骤，它执行对包括压缩内容和压缩内容的扩展处理程序在内的内容数据的内容数据分析并执行从内容数据中对压缩内容和扩展处理程序的抽取处理；扩展处理步骤，它用包括在因内容数据分析部的分

析而获得的内容数据中的扩展处理程序来执行对包括在内容数据中的内容数据的扩展处理。

本发明的程序提供介质例如是这样一种介质，它将计算机可读形式的计算机程序提供给能执行多种程序代码的通用计算机系统。所述介质的一种形式是诸如 CD、FD 或 MO 之类的存储介质或者是诸如网络之类的传输介质，但没有特定的限制。

这种程序提供介质限定了计算机程序与提供介质之间的结构或功能性合作关系，以便实现计算机系统上的计算机程序的预定功能。换句话说，通过用提供介质将计算机程序安装到计算机系统中而在计算机系统上显示出合作操作，并且，可以获得与本发明其它方面相类似的操作效果。

根据后述本发明实施例和附图可以详细说明和看出本发明的其它目的、特征和优点。

如上所述，依照本发明的数据处理设备和方法以及数据验证值给出方法，将生成为整体性检查值的部分整体性检查值用于比较过程以便验证部分数据，所述部分整体性检查值可用于通过将内容数据划分成多个部分而获得的包含有一个或多个部分数据的部分数据集，并且，将用于验证部分整体性检查值数值集的部分整体性检查值验证整体性检查值用于比较过程，以便验证与构成部分整体性检查值数值集的多个部分整体性检查值相对应的多个部分数据集的全部，所述部分整体性检查值数值集包括多个部分整体性检查值的组合。因此，与将单个整体性检查值给予整个内容数据的结构相比，可作到部分验证，并且，全部的验证过程因使用了部分整体性检查值而是有效的。

另外，依照本发明的数据处理设备和方法以及数据验证值给出方法，按着如何使用内容数据例如是下载数据还是再现数据来执行验证过程；例如，可略去对不可能篡改的数据部分的验证过程。所以，能按着如何使用数据而进行有效的验证。

此外，本发明的数据处理设备和数据处理方法是按这样方式配置的：执行诸如数据加密、数据解密、数据验证、鉴别处理和签名处理之类的加密处理所需的个别密钥不存储在存储部内，相反，生成这些个别密钥的主密钥存储在存储部内，所述数据处理设备的加密处理部从存储部中按需抽取与诸如加密密钥和鉴别密钥之类个别密钥相对应

的主密钥、根据抽出的设备或数据的主密钥和标识数据执行应用 DES 算法等的加密处理并生成诸如加密密钥和鉴别密钥之类的个别密钥，从而，本发明能消除个别密钥本身从存储部中泄露的可能性并提高加密处理系统的安全性，因为，获得个别密钥需要诸如个别密钥生成算法和主密钥、设备或数据的标识数据的信息之类的多种信息。而且，即使因某些原因泄露了个别密钥，受破坏的范围也限于个别密钥的范围，这不会导致整个系统崩溃。

再有，本发明的数据处理设备和数据处理方法是按这样方式配置的：根据设备或数据的标识数据顺序地生成个别密钥，这会消除将用于个别设备的密钥列表保存在控制设备内的需要，从而便于系统控制并提高安全性。

另外，依照本发明的数据处理设备和内容数据生成方法，将非法设备标识数据信息存储在内容数据中，在用记录器/再现器使用内容之前执行非法设备列表与试图使用这些内容检查值记录器/再现器的记录器/再现器标识符之间的比较，并且，在比较结果展示出非法设备列表的某些条目与记录器/再现器标识符相匹配的情况下，就停止随后的处理过程例如内容数据解密、下载或再现处理等，因此，能防止具有非法获得的密钥的再现器等非法地使用内容。

另外，本发明的数据处理设备、数据处理方法和内容数据生成方法采用这样的结构，它能使内容数据包括一道用于内容数据中非法设备列表的检查值，从而能防止篡改列表本身并提供有提高了的安全性的内容数据使用结构。

再有，本发明的数据处理设备和数据处理方法能使得诸如记录器/再现器和 PC 之类的数据处理设备存储为数据处理设备所专用的设备专用密钥以及为使用内容数据的其它数据处理设备所共用的系统共用密钥，从而能根据内容使用限制对内容进行处理。所述数据处理设备根据内容使用限制有选择地使用这两种密钥。例如，在内容仅为数据处理设备所用的情况下，就使用为数据处理设备所专用的密钥，而在内容也可为其它系统所用的情况下，就生成用于内容数据的检查值并用系统共用密钥执行比较处理过程。仅在形成了比较时才能对加密的数据进行解密和再现，从而能根据诸如内容仅用于数据处理设备或内容为系统所共用等之类内容使用限制进行处理。

再有，本发明的数据处理设备、数据处理方法和内容数据验证值赋值方法配置成能生成内容块数据单元的内容检查值、对所生成的内容检查值进行比较处理、根据要加以验证的内容块数据生成内容中间值并通过应用内容检查值生成密钥的加密处理来生成内容检查值，从而与通常的处理过程相比能有效地对整个数据进行验证。

此外，本发明的数据处理设备、数据处理方法和内容数据验证值赋值方法能依照下载处理过程和再现处理过程等在内容块单元中进行验证并有简化的验证处理过程，从而能根据使用模式提供有效的验证。

再有，由于本发明的数据处理设备、内容数据生成方法和数据处理方法具有这样的结构，该结构配备有内容数据中的多个内容块并能对各内容块单元进行加密处理，而且，本发明的数据处理设备、内容数据生成方法和数据处理方法还具有这样的结构，其中，对用于内容加密的密钥作进一步加密并将该密钥存储进头标部，所以，即使例如存在有多个内容块并且需要加密处理的块和不需加密处理的块相混合，也能够具有将各块连起来的任意数据结构。

此外，依照本发明的数据处理设备、数据处理系统和数据处理方法，通过使内容块的结构是规则结构，例如是具有均匀数据长度的结构或加密块和非加密（无格式文本）块是交替设置的结构，可迅速地执行内容块的解密过程和类似的过程，并且，可以提供适于进行处理的与内容数据的内容相对应的加密内容数据，例如对音乐数据进行再现和类似的处理。

再有，所述数据处理设备、数据处理方法和内容数据生成方法可在内容是压缩声音数据、图像数据或类似数据的情况下有效地执行再现处理。也就是说，通过使内容数据的结构是其中压缩数据和扩展处理程序结合在一起的结构，可以在再现处理设备内进行扩展处理，并将属于压缩内容数据的扩展处理程序应用于该扩展处理，并且，可以避免这样的情况，其中，扩展处理程序不存在于再现处理设备内，从而不能进行再现。

而且，依照数据处理设备、数据处理方法和内容数据生成装置，由于内容数据的结构具有这样的结构，其中，所述再现处理设备根据头标信息确定能应用于压缩内容数据的扩展处理程序，并且，所述再

现处理设备还从可访问的记录介质或类似装置中检索出可应用的程序，并且通过使内容数据是压缩数据和存储有压缩处理程序类型的头标部的组合而执行扩展处理，或者，如果所述内容具有扩展处理程序、扩展处理程序和存储有上述程序类型的头标部的组合，则不需要由用户来执行程序检索处理，从而，可以进行有效的再现处理。

附图说明

图 1 是示出了常规数据处理系统的结构的图；

图 2 是示出了应用了本发明数据处理设备的结构的图；

图 3 是示出了应用了本发明数据处理设备的结构的图；

图 4 是示出了介质或通信路径上内容数据的数据格式的图；

图 5 是示出了包含在内容数据的头标中的使用策略的图；

图 6 是示出了包含在内容数据的头标中的块信息的图；

图 7 是示出了用 DES 的电子签名生成方法的图；

图 8 是示出了用三重 DES 的电子签名生成方法的图；

图 9 是用于说明三重 DES 方面的图；

图 10 是示出了部分使用三重 DES 的电子签名生成方法的图；

图 11 是示出了电子签名生成的流程；

图 12 是示出了电子签名生成的流程；

图 13 是用于说明用对称密码翻译技术的相互鉴别处理过程序列的图；

图 14 是用于说明公共密钥证书的图；

图 15 是用于说明用非对称密码翻译技术的相互鉴别处理过程顺列的图；

图 16 是示出了用椭圆曲线密码翻译的加密过程的流程的图；

图 17 是示出了用椭圆曲线密码翻译的解密过程的流程的图；

图 18 是示出了如何将数据保存在记录和再现设备上的图；

图 19 是示出了如何将数据保存在记录设备上的图；

图 20 是示出了记录和再现设备与记录设备之间相互鉴别流程的图；

图 21 是示出了记录和再现设备的主密钥与记录设备的相应主密钥之间关系的图；

图 22 是示出了内容下载过程的流程的图；

图 23 是用于说明生成整体性检查值 A: IVCa 的方法的图;

图 24 是用于说明生成整体性检查值 B: IVCa 的方法的图;

图 25 是用于说明生成总体整体性检查值及记录和再现设备所独有的整体性检查值;

图 26 是示出了存储在记录设备中的内容数据格式的图(本地化字段=0);

图 27 是示出了存储在记录设备中的内容数据格式的图(本地化字段=1);

图 28 是示出了内容再现过程的流程的图;

图 29 是用于说明记录设备执行命令的方法的图;

图 30 是用于说明记录设备在内容存储过程中执行命令的方法的图;

图 31 是用于说明记录设备在内容再现过程中执行命令的方法的图;

图 32 是用于说明内容数据格式类型 0 的结构的图;

图 33 是用于说明内容数据格式类型 1 的结构的图;

图 34 是用于说明内容数据格式类型 2 的结构的图;

图 35 是用于说明内容数据格式类型 3 的结构的图;

图 36 是用于说明生成用于格式类型 0 的内容整体性检查值 IDVi 的方法的图;

图 37 是用于说明生成用于格式类型 1 的内容整体性检查值 IDVi 的方法的图;

图 38 是用于说明用于格式类型 2 和 3 的总体整体性检查值及记录和再现设备所独有的整体性检查值的图;

图 39 是示出了用于下载格式类型 0 或 1 的内容的过程的图;

图 40 是示出了用于下载格式类型 2 的内容的过程的图;

图 41 是示出了用于下载格式类型 3 的内容的过程的图;

图 42 是示出了用于再现格式类型 0 的内容的过程的图;

图 43 是示出了用于再现格式类型 1 的内容的过程的图;

图 44 是示出了用于再现格式类型 2 的内容的过程的图;

图 45 是示出了用于再现格式类型 3 的内容的过程的图;

图 46 是用于说明内容生成器和内容验证器生成整体性检查值并用

它们进行验证的方法的图(1);

图47是用于说明内容生成器和内容验证器生成整体性检查值并用它们进行验证的方法的图(2);

图48是用于说明内容生成器和内容验证器生成整体性检查值并用它们进行验证的方法的图(3);

图49是用于说明用主密钥个别生成多种密钥的方法的图;

图50是示出了内容提供者和用户所执行的过程的实例以及用主密钥个别生成多种密钥的方法的图(实例1);

图51是示出了内容提供者和用户所执行的过程的实例以及用主密钥个别生成多种密钥的方法的图(实例2);

图52是用于说明用不同的主密钥执行本地化的结构的图;

图53是示出了内容提供者和用户所执行的过程的实例以及用主密钥个别生成多种密钥的方法的图(实例3);

图54是示出了内容提供者和用户所执行的过程的实例以及用主密钥个别生成多种密钥的方法的图(实例4);

图55是示出了内容提供者和用户所执行的过程的实例以及用主密钥个别生成多种密钥的方法的图(实例5);

图56是示出了用单DES算法存储带有应用了的三重DES的密码翻译密钥的过程的流程的图;

图57是示出了基于优先权的内容再现流程(实例1)的图;

图58是示出了基于优先权的内容再现流程(实例2)的图;

图59是示出了基于优先权的内容再现流程(实例3)的图;

图60是用于说明在内容再现过程中执行对压缩数据进行解密(解压缩)的过程的结构的图;

图61是示出了内容结构的实例的图(实例1);

图62是内容结构的实例1中的再现流程的图;

图63是示出了内容结构的实例的图(实例2);

图64是内容结构的实例2中的再现流程的图;

图65是示出了内容结构的实例的图(实例3);

图66是内容结构的实例3中的再现流程的图;

图67是示出了内容结构的实例的图(实例4);

图68是内容结构的实例4中的再现流程的图;

图 69 是用于说明生成和存储保存数据的图;

图 70 是示出了存储保存数据的过程的实例(实例 1)的流程的图;

图 71 是示出了存储并再现保存数据过程中使用的数据管理文件的结构的图(实例 1);

图 72 是示出了再现保存数据过程的实例(实例 1)的流程的图;

图 73 是示出了存储保存数据过程的实例(实例 2)的流程的图;

图 74 是示出了存储再现数据过程的实例(实例 2)的流程的图;

图 75 是示出了存储保存数据过程的实例(实例 3)的流程的图;

图 76 是示出了存储并再现保存数据过程中使用的数据管理文件的结构的图((实例 2);

图 77 是示出了再现保存数据过程的实例(实例 3)的流程的图;

图 78 是示出了存储保存数据过程的实例(实例 4)的流程的图;

图 79 是示出了再现保存数据过程的实例(实例 4)的流程的图;

图 80 是示出了存储保存数据过程的实例(实例 5)的流程的图;

图 81 是示出了存储并再现保存数据过程中使用的数据管理文件的结构的图((实例 3);

图 82 是示出了再现保存数据过程的实例(实例 5)的流程的图;

图 83 是示出了存储保存数据过程的实例(实例 5)的流程的图;

图 84 是示出了存储并再现保存数据过程中使用的数据管理文件的结构的图((实例 4);

图 85 是示出了再现保存数据过程的实例(实例 6)的流程的图;

图 86 是用于解释排除无效内容用户(撤消)的结构的图;

图 87 是示出了用于排除无效内容用户(撤消)的过程(实例 1)的流程的图;

图 88 是示出了用于排除无效内容用户(撤消)的过程(实例 2)的流程的图;

图 89 是用于说明保密芯片(实例 1)的结构的图;

图 90 是示出了用于生产保密芯片的方法的流程的图;

图 91 是用于说明保密芯片(实例 2)的结构的图;

图 92 是示出了用于将数据写入保密芯片(实例 2)的过程的流程的图;

图 93 是示出了用于检查保密芯片中写入的数据的过程的流程的

图。

标号说明:

106、主 CPU
107、RAM
108、ROM
109、AV 处理器部
110、输入处理部
111、PIO
112、SIO
300、记录和再现设备
301、控制部
302、密码翻译处理部
303、记录设备控制器
304、读取部
305、通讯部
306、控制部
307、内部存储器
308、加密/解密部
401、密码翻译处理部
402、外部存储器
403、控制部
404、通讯部
405、内部存储器
406、加密/解密部
407、外部存储器控制部
500、介质
600、通讯装置
2101、2102、2103、记录和再现设备
2104、2105、2106、记录设备
2901、命令号管理部
2902、命令寄存器
2903、2904、鉴别标志
3001、扬声器
3002、监视器
3090、存储器
3091、内容分析部
3092、数据存储部
3093、程序存储部
3094、压缩解压缩处理部
7701、内容数据
7702、撤消列表
7703、列表检查值
8000、保密芯片
8001、处理部
8002、存储部
8003、模式信号线
8004、命令信号线
8201、读写区域
8202、只写区域

具体实施方式

以下说明本发明的实施例。说明按以下项目次序进行:

(1)、数据处理设备的结构

(2)、内容数据格式

(3)、适用于本发明数据处理设备的密码翻译处理过程概要

(4)、存储在记录和再现设备中的数据的结构

(5)、存储在记录设备中的数据的结构

(6)、记录和再现设备与记录设备之间的相互鉴别处理过程

(6-1)、相互鉴别过程概要

(6-2)、在相互鉴别过程中切换至密钥块

(7)、用于从记录和再现设备中下载至记录设备的过程

(8)、记录和再现设备所执行的用于再现来自记录设备的信息的过程

(9)、相互鉴别之后的密钥交换过程

(10)、多种内容数据格式以及与各格式相对应的下载和再现过程

(11)、内容提供者所执行的用于生成检查值(ICV)的过程方面

(12)、基于主密钥的密码翻译处理过程密钥生成结构

(13)、在密码翻译处理过程中控制密码翻译处理程度

(14)、基于内容数据处理策略中优先权的程序启动过程

(15)、内容结构和再现(解压缩)过程

(16)、用于生成并将保存数据存储在记录设备内并再现来自记录设备的保存数据的过程

(17)、用于排除(撤消)非法设备的结构

(18)、保密芯片的结构以及保密芯片的生产方法

(1)、数据处理设备的结构

图 2 示出了一框图，该框图示出了本发明数据处理设备的一个实施例的总体结构。该数据处理结构的主要组件是记录和再现设备 300 以及记录设备 400。

记录和再现设备 300 包括例如个人计算机(PC)、游戏设备或类似设备。记录和再现设备 300 具有：控制部 301，它用于实现统一控制，包括控制记录和再现设备 300 与记录设备 400 之间在记录和再现设备 300 中密码翻译处理过程中的通信；记录和再现设备密码翻译处理部 302，它负责整个的密码翻译处理过程；记录设备控制器 303，它用于执行与记录设备 400 的鉴别过程，以便读写数据，所述记录设备 400 与上述记录和再现设备相连；读取部 304，它用于至少从诸如 DVD 之类的介质 500 中读取数据；以及，通信部 305，它用于将数据传送至外部或从外部接收数据，如图 2 所示。

记录和再现设备 300 将内容数据下载和再现至记录设备 400 并下

载和再现来自记录设备的内容数据，记录设备受控于控制部 301。记录设备 400 是这样的存储介质，它能最佳地安装到记录和再现设备 300 上并从记录和再现设备 300 上拆除，例如是存储卡，所述存储具有外部存储器 402，它包括诸如 EEPROM 或按块擦除存储器、硬盘或带电池的 RAM 之类的非易失性存储器。

记录和再现设备 300 具有：作为接口的读取部 304；可向其输入存储器在图 2 左端所示的存储介质即 DVD、CD、FD 或 HDD 内的内容数据；以及，作为接口的通信部 305，可向其输入发布自诸如因特网之类的网络的内容数据，以便接收来自外部的内容输入。

记录和再现设备 300 具有密码翻译处理部 302，以便执行鉴别过程、加密和解密过程、数据验证过程以及在下载通过读取部 304 或通信部 306 从外部输入给记录设备 400 的内容数据时或在再现和执行来自记录设备 400 的内容数据时的其它过程。密码翻译处理部 302 包括：控制部 306，它用于控制整个的密码翻译处理部 302；内部存储器 307，它保存诸如密钥之类用于密码翻译处理过程的信息，所述信息经过处理，从而能防止很容易地从外部读取数据；以及，加密/解密部 308，它用于执行加密和解密过程、生成并验证鉴别数据、生成随机数等。

在例如记录设备 400 安装在记录和再现设备 300 内或执行用于诸如记录和再现设备密码翻译处理部 302 的加密/解密部 308 与记录设备密码翻译处理部 401 的加密/解密部 406 之间的相互鉴别之类的多种过程的仲裁过程、整体性检查值比较过程以及加密和解密过程时，控制部 301 将初始化命令通过记录设备控制器 303 传给记录设备 400。这些过程中的每一个过程都将在后续部分中作详细说明。

密码翻译处理部 302 执行鉴别过程、加密和解密过程、数据验证过程以及如前所述的其它过程并具有密码翻译处理部控制部 306、内部存储器 307 以及加密/解密部 308。

密码翻译处理控制部 306 对诸如记录和再现设备 300 所执行的鉴别过程及加密/解密过程之类的整个密码翻译处理过程、例如在记录和再现设备 300 与记录设备 400 之间执行的鉴别过程业已完成时设置鉴别完成标志的过程、命令执行在记录和再现部密码翻译处理部 302 的加密/解密部 308 中执行的各种过程例如下载过程和用于生成再现内容数据的整体性检查值的过程以及命令执行生成各种密钥数据的过程进

行控制。

如以下详细说明的那样，内部存储器 307 存储密钥数据、标识数据以及其它诸如相互鉴别过程、整体性检查值比较过程以及在记录和再现设备 300 中执行的加密和解密过程之类多种过程所需的其它数据。

加密/解密部 308 在将输入内容数据从外部下载至记录设备 400 或再现并执行存储在记录设备 400 内的内容数据时用存储器在内部存储器 307 中的密钥数据和类似数据去执行鉴别过程、加密和解密过程、生成并验证预定的整体性检查值或电子签名、验证数据、生成随机数等。

在这种情况下，记录和再现设备密码翻译处理部 302 的保存诸如密码翻译密钥之类的重要信息从而必须配置成不能很容易地从外部读出数据。因此，密码翻译处理部配置成一防篡改存储器，其特征在于，能防止外部无效读取，因为，该存储器包括半导体芯片，它能基本上拒绝外部访问并具有多层结构、在铝或类似材料制成的哑层之间切换或设置在最低层上的内部存储器以及狭窄范围的操作电压和/或频率。以下将详细说明这一结构。

除密码翻译处理过程以外，记录和再现设备 300 包括主中央处理器(CPU)106、RAM(随机存取存储器)107、ROM(只读存储器)108、AV 处理部 109、输入接口 110、PIO(并行 I/O)接口 111 和 SIO(串行 I/O)接口 112。

主中央处理器(CPU)106、RAM(随机存取存储器)107、ROM(只读存储器)108 是这样的组件，它用作记录和再现设备 300 的主体的控制系统并主要用作用于再现记录和再现设备密码翻译处理部 302 所解密的数据的再现处理部。例如，主中央处理器(CPU)106 在控制部 301 的控制下对诸如将从记录设备中读出并进行解密的内容数据输出给 AV 处理部 109 之类的再现和执行内容进行控制。

RAM107 用作用 CPU106 所执行的过程的主存储存储器并用作用于这些过程的工作区。ROM108 存储器用于启动由 CPU106 所启动的 OS 或类似系统的基本程序以及其它数据。

AV 处理部 109 具有数据压缩和解压缩处理装置，具体地说是 MPEG2 解码器、ATRAC 解码器、MP3 解码器或类似解码器，以执行用于将数据

输出给诸如显示容或扬声器(未示出)之类安装或连接于记录和再现设备主体的数据输出设备的过程。

输入接口 110 将来自诸如控制器、键盘和鼠标之类的多种连接输入装置的输入数据输出给主 CPU106。主 CPU106 按着用户根据正执行的游戏程序或类似程序通过控制器发出的命令进行处理。

PIO(并行 I/O)接口 111 和 SIO(串行 I/O)接口 112 用作用于存储卡或游戏盒的存储装置并用作便携电子装置或类似装置的连接装置。

主 CPU106 还在保存为保存数据、设置数据或用于正执行的游戏或类似程序的类似操作时进行控制。在这一过程中，将存储的数据传给控制部 301，它能使密码翻译处理部 302 按需执行对保存数据的密码翻译处理，然后将加密数据存储器到记录设备 400 内。以下将详细说明这些密码翻译处理过程。

记录设备 400 是这样的存储介质，它能最佳地安装到记录和再现设备 300 并从记录和再现设备 300 中拆下，而且包括例如存储卡。记录设备 400 具有密码翻译处理部 401 和外部存储器 402。

记录设备密码翻译处理部 401 执行相鉴别过程、加密和解密过程、数据验证过程以及在从记录和再现设备 300 中下载内容数据或将来自记录设备 400 的内容数据再现至记录和再现设备 300 时记录和再现设备 300 与记录设备 400 之间的其它过程并具有控制部、内部存储器、加密/解密部和与记录和再现设备 300 的密码翻译处理部相类似的其它装置。图 3 中示出了细节。外部存储器 402 包括非易失性存储器，它包括诸 EEPROM 之类的按块擦除存储器、硬盘、或带电池的 RAM 或类似装置，以便存储加密的内容数据或类似数据。

图 3 是概略示出了输入自介质 500 和通信装置 600 的数据的结构的图，所述介质 500 和通信装置 600 是数据提供装置，本发明的数据处理设备从其接收数据，图 3 重点在于记录和再现设备 300 的结构以及用于记录设备 400 中密码翻译处理过程的结构，所述记录和再现设备 300 从内容提供装置 500 或 600 中接收内容输入。

介质 500 例如是光盘介质、磁盘介质、磁带介质、半导体介质或类似介质。通信装置 600 是诸如因特网、电缆或卫星通信装置之类的数据通信装置。

在图 3 中，记录和再现设备 300 验证介质 500 或通信装置 600 输

入的数据即满足图 3 所示预定格式的内容，并将验证过的内容存储到记录设备 400 中。

如在介质 500 和通信装置 600 的部分所示，内容数据具有以下组成：

内容 ID：作为内容数据标识符的内容 ID。

使用策略；使用策略包含内容数据的构成信息，例如，构成内容数据的头标部和内容部的长度、格式版本、指示内容是程序还是数据的内容类型、指示内容仅可用于下载该内容的设备还是也可用于其它设备的本地化字段。

块信息表：块信息表包括内容块的数量、块长度、指示存在加密的加密标志以及其它内容。

密钥数据：密钥数据包括用于对上述块信息表进行加密的加密密钥、用于对内容块加密的内容密钥以及类似密钥。

内容块：内容块包括程序数据、音乐或图像数据或者要加以实际再现的其它数据。

以下将参照图 4 和后续附图详细说明内容数据。

内容数据由内容密钥(以下称为“Knon”)来加密并被从介质 500 或通信装置 600 提供给记录和再现设备 300。可通过记录和再现设备 300 将内容存储在记录设备 400 的外部存储内。

例如，记录设备 400 在将包含在内容数据中的内容、作为头标信息包含在内容数据中的块信息表、与诸如内容密钥 Kcon 之类多种密钥有关的信息存储在外部存储器 402 之前使用它所独有的存储在内部存储器 405 中的密钥(以下称为“存储密钥”(Kstr))来对这些数据进行加密。为了将内容数据从记录和再现设备 300 下载至记录设备 400 或者使记录和再现设备 300 再现存储在记录设备 400 中的内容数据，需要诸如设备与内容数据加密和解密过程之间的相互鉴别之类的预定过程。以下将详细说明这些过程。

记录设备 400 具有密码翻译处理部 401 和外部存储器 402，密码翻译处理部 401 具有控制部 403、通信部 404、内部存储 405、加密/解密部 406 以及外部存储器控制部 407。

记录设备 400 负责整个的密码翻译处理、控制外部存储器 402 并包括：记录设备密码翻译处理部 401，它用于解释来自记录和再现设备

300 的命令并执行处理过程；以及，外部存储器 402，它保存有内容等。

记录设备密码翻译处理部 401 具有：控制部 403，它用于控制整个记录设备密码翻译处理部 401；通信部 404，它用于将数据传给记录和再现设备 300 并接收来自记录和再现设备 300 的数据；内部存储器 405，它保存有诸如密钥之类用于密码翻译处理过程并业已被处理以便防止从外部很容易读出数据的信息；加密/解密部 406，它用于执行加密和解密处理过程、生成并验证鉴别数据、生成随机数等；以及，外部存储器控制部 407，它用于从外部存储器 402 中读出数据并将数据写至外部存储器 402。

控制部 403 对诸如记录设备 400 所执行的鉴别过程以及加密/解密过程之类的整个密码翻译处理过程例如在记录和再现设备 300 与记录设备 400 之间执行的鉴别过程业已完成时设置鉴别完成标志的过程、命令执行密码翻译处理部 401 的加密/解密部 406 中执行的多种过程例如下载过程和用于生成再现内容数据的整体性检查值的过程以及命令执行用于生成多种密钥数据的过程进行控制。

内部存储器 405 包括一存储器，它具有多个块以存储多组密钥数据、标识数据或诸如记录设备 400 如以下详细所述那样执行的相互鉴别过程、整体性检查值比较过程以及加密和解密过程之类的多种过程所需的其它数据。

记录设备密码翻译处理部 401 的内部存储器 405 与前述记录和再现设备密码翻译处理部 302 的内部存储器 307 相类似保存有诸如密码翻译密钥之类的重要信息，因此必须配置成不能从外部很容易地读取其数据。所以，记录和再现设备 400 的密码翻译处理部 401 的特征在于能防止外部无效读取，因为，它包括半导体芯片，此芯片能基本上拒绝外部访问并具有多层结构、在铝或类似材料制成的哑层之间切换或设置在最低层上的内部存储器以及狭窄范围的操作电压和/或频率。这方面，记录和再现设备密码翻译处理部 302 可是以这样的软件，它配置成能防止用于密钥的保密信息很容易地泄露给外部。

加密/解密部 406 在从记录和再现设备 300 中下载内容数据、再现存储在记录设备 400 的外部存储器 402 中的内容数据或执行记录和再现设备 300 与记录设备 400 之间的相互验证时用存储在内部存储器 405 中的密钥数据或类似数据执行数据验证过程、加密和解密过程、生成

和验证预定整体性检查值或电子签名、生成随机数等。

通信部 404 与记录和再现设备 300 的记录设备控制器 303 相连，以便下载或再现内容数据或或在按记录和再现设备 300 的控制部 301 的控制或记录设备 400 的控制部 403 的控制而在相互鉴别过程中在记录和再现设备 300 与记录设备 400 之间传递传送数据。

(2) 内容数据格式

以下用图 4 至图 6 说明存储在本发明系统的介质 500 内的或在数据通信装置 600 上传送的数据的数据格式。

图 4 所示的结构示出了整个内容数据的格式，图 5 所示的结构示出了部分地构成了内容数据的头标部的“使用策略”的细节，图 6 所示的结构示出了部分地构成了内容的头标部的“块信息表”的细节。

以下说明应用于本发明系统的数据格式的代表性实例，但是，诸如与游戏程序相对应的格式以及适用于实时处理音乐数据或类似数据的格式之类的不同类型的数据格式也可用于本系统。以下在“(10) 多种内容数据格式以及与各格式相对应的下载和再现过程”中将详细说明这些格式。

在图 4 所示的数据格式中，灰色所示的条目表示加密的数据，双框封起的条目表示篡改检查数据、白色所示的其它条目表示未加密的老格式文本数据。加密部的加密密钥示于双框的左侧。在图 4 所示的实例中，内容部的某些块(内容块数据)包含加密的数据，而其它块则包含非加密的数据。这种形式随内容数据而变，可对包含在数据中的所有内容块数据进行加密。

如图 4 所示，将数据格式划分成头标部和内容部，头标部包括内容 ID、使用策略、整体性检查值 A〈以下称为“ICVa”〉、块信息表密钥(以下称为“Kbit”)、内容密钥 Kcon、块信息表(以下称为“BIT”)、整体性检查值 B(ICVb)以及总体整体性检查值(ICVt)，内容部包括多个内容块(例如，加密的和非加密的内容)。

在这种情况下，个别信息表示用于标识内容的内容 ID。使用策略包括表示头标部长度的头标长度、表示内容部长度的内容长度、表示格式版本信息的格式版本、表示格式类型的格式类型、表示内容类型即是程序还是数据的内容类型、如果内容类型是程序则表示启动优先权的操作优先权、表示仅可将按这种格式下载的内容用于下载该内容

的设备还是也可用于其它类似设备的本地化字段、表示是否可将按这种格式下载的内容从下载该内容的设备拷贝至其它类似设备的拷贝许可、表示是否可将按这种格式下载的内容从下载该内容的设备移至至其它类似设备的移动许可、表示用于对内容部中的内容块进行加密的算法的加密算法、表示控制用于对内容部中的内容进行加密的算法的方法的加密模式、以及表示用于生成整体性检查值的方法的整体性检查方法，详细如图 5 所示。

上述记录在使用策略中的数据条目仅仅是示例性的，可根据相应的内容数据方面记录多种使用策略信息。以下在例如“(17)用于排除(撤消)非法设备”中详细说明标识符。还可以形成一种能排除非法设备通过将非法记录和再现设备的内容记录为数据并通过检查开始使用的时间来使用内容的结构。

整体性检查值 A ICVa 用于验证内容 ID 或使用策略未被篡改。该值用作检查值，它用于部分数据而不是整个内容数据，也就是说，用作部分整体性检查值。数据块信息表密钥 Kbit 用于对块信息表进行加密，内容密钥 Kcon 用于对内容块进行加密。块信息表密钥 Kbit 和内容密钥利用介质 500 和通信装置 600 上的发布密钥(以下称为“Kdis”)进行加密。

图 6 详细地示出了块信息表。图 6 中的块信息表包括所有利用图 4 所示块信息表密钥 Kbit 加以加密的数据。块信息表包括块号，它表示 N 个内容块上的内容块和信息的号码，如图 6 所示。内容块信息表包括块长度、表示块是否以被加密的加密标志、表示是否必须计算整体性检查值的 ICV 标志以及内容整体性检查值(ICVi)。

内容整体性检查值用于验证各内容块尚未被篡改。以下在“(10)多种内容数据格式以及与各格式相对应的下载和再现过程”中将说明用于生成内容整体性检查值的方法的具体实例。用发布密钥 Kdis 对用于对块信息表加密的块信息表密钥 Kbit 作进一步的加密。

继续说明图 4 中的数据格式。整体性检查值 B ICVb 用于验证块信息表密钥 Kbit、内容密钥 Kcon 以及块信息表未被篡改。该值用作检查值，它用于部分数据而不是整个内容数据，也就是说，用作部分整体性检查值。总体整体性检查值 ICVt 用于验证整体性检查值 ICVa 和 ICVb、用于各内容块的整体性检查值 ICVi(如果已作了设置的话)、部

分整体性检查值或者所有要加以检查的数据未被篡改。

在图 6 中，可任意地设置块长度、加密标志和 ICV 标志，但也可以形成某些规则。例如，可在固定长度上重复加密的和无格式文本区域，可对所有的内容数据解密，或者对块信息表 BIT 进行压缩。此外，为了使不同的内容密钥 Kcon 用于不同的内容块，内容密钥 Kcon 包含在内容块内而不是包含在头标部内。以下在“(10)多种内容数据格式以及与各格式相对应的下载和再现过程”中将详细说明内容数据格式的实例。

(3)适用于本发明数据处理设备的密码翻译处理过程概要

以下说明适用于本发明数据处理设备的多种密码翻译处理过程的方面。在“(3)适用于本发明数据处理设备的密码翻译处理过程概要”中对密码翻译处理过程的说明对应于密码翻译处理过程的方面概要，例如“a.记录和再现设备与记录设备之间的鉴别过程”、“b.用于加载内容的设备的下载过程”、“c.用于再现存储在记录设备内的内容的过程”，以下将具体说明的本发明数据处理设备所执行的多种过程都是以该概要为基础的。在条目(4)和后续条目中分别详述记录和再现设备 300 和记录设备 400 所执行的具体过程。

按以下次序说明适用于数据处理设备的密码翻译处理过程概要:

(3-1) 基于共用密钥密码系统的消息鉴别

(3-2) 基于公共密钥密码系统的电子签名

(3-3) 基于公共密钥密码系统的电子签名验证

(3-4) 基于共用密钥密码系统的相互鉴别

(3-5) 公共密钥证书

(3-6) 基于公共密钥密码系统的相互鉴别

(3-7) 用椭圆曲线密码翻译的加密过程

(3-8) 用椭圆曲线密码翻译的解密过程

(3-9) 随机数生成过程

(3-1)基于共用密钥密码系统的消息鉴别

首先，说明一种使用共用密钥加密方法来生成篡改检测数据的过程。该篡改检测数据被附加到要进行篡改检测的数据上，以便检查篡改和鉴别生成器。

例如，将图 4 所述用双框封起的数据结构中的整体性检查值 A 和 B

以及总体整体性检查值、存储在图 6 所示块信息表中的各块内的内容检查值以及类似的值生成为篡改检测数据。

这里，作为用于生成并处理电子签名数据的方法的一个实例，说明 DES 的使用，DES 是一种共用密钥密码系统。除 DES 以外，本发明还可将例如 FEAL(快速加密算法)或 AES(高级加密标准)(美国下一代标准密码翻译)用作类似的以共用密钥密码系统为基础的过程。

参照图 7 说明用通用 DES 生成电子签名的方法。首先，在生成电子签名之前，将要把电子签名附加给它的消息分成 8 字节的集合(以下将划分出来的消息段称为“M1，M2，...MN”)。对初始(以下称为“IV”)和 M1 作异或操作(结果称为“I1”)。然后，将 I1 输入给 DES 加密部，它用密钥(以下称为“K1”)对 I1 进行加密(输出称为“E1”)。此后，对 E1 和 M2 作异或操作，将 I2 输入给 DES 加密部，它用密钥 K1 对 I1 进行加密(输出称为“E2”)。重复这一过程以便对通过划分所获得的所有消息。最终的输出 EN 就是电子签名。该值一般称为“MAC(消息鉴别码)”，它用于检查消息的篡改情况。此外，这种用于将加密的文本链起来的系统称为“CBC(加密块链接)模式”。

图 7 所示的生成实例中的 MAC 值输出可用作图 4 所示的用双框封起的数据结构中的整体性检查值 A 或 B 或总体整体性检查值以及存储在图 6 所示块信息表中各块内的内容检查值 ICV1 至 ICVN。在验证 MAC 值时，验证器用与用来在开始生成 MAC 值相类似的方法生成 MAC 值，如果获得了相同的值，则可确定验证成功。

而且，在图 7 所示的实例中，初始值 IV 与头 8 字节消息 M1 作异或运算，但是，初始值 IV 可以是零，从而不进行异或运算。

图 8 示出了用于生成 MAC 值的方法的结构，所述方法与图 7 所示的 MAC 值生成方法相比具有改进了的安全性。图 8 示出了这样的实例，其中，不是用图 7 中的单 DES 而是用三重 DES 来生成 MAC 值。

图 9A 和 9B 示出了图 8 所示的各三重 DES 组件的详细结构的实例。如图 9 所示，存在有三重 DES 的结构的两种不同方面。图 9(a)示出了使用两个密码翻译密钥的实例，其中，按用密钥 1 的加密处理、用密钥 2 的解密处理以及用密钥 1 的加密处理的次序进行处理。按 K1、K2 和 K1 的次序使用两种类型的密钥。图 9(b)示出了用三个密码翻译密钥的实例，其中，按用密钥 1 的加密处理、用密钥 2 的加密处理和用密

钥 3 的加密处理的次序进行处理。按 K1、K2 和 K3 的次序使用三种类型的密钥。因此，可以连续地执行多次处理，以便与单 DES 相比提高保密程度。但是，三重 DES 结构具有需要三倍于单 DES 的处理时间。

图 10 示出了通过改进图 8 和 9 所述的三重 DES 结构而获得的 MAC 值生成结构的实例。在图 10 中，从要增加有签名的消息串的开始到结束的用于各消息的加密过程是以单 DES 为基础的，而只有用于最后消息的加密过程是以图 9(a)所示的三重 DES 结构为基础的。

图 10 所示的结构能将生成用于消息的 MAC 值所需的时间降低至几乎等于基于单 DES 的 MAC 值生成过程所需的时间，保密性与基于单 DES 的 MAC 值相比有所提高。而且，用于最后消息的三重 DES 结构如图 9(b)所示。

(3-2)基于公共密钥密码系统的电子签名

业已说明了在将公用密钥加密系统用作加密系统的情况下的用于生成电子签名数据的方法，以下参照图 11 说明在将共用密钥密码系统用作加密系统的情况下的用于生成电子签数据名的方法。图 11 所述的过程与用椭圆曲线数字签名算法(EC-DSA) IEEE P1363/D3 的生成电子签名数据的流程相对应。以下说明将椭圆曲线密码翻译(以下称为“ECC”)用作公共密钥密码翻译的实例。除椭圆曲线密码翻译以外，本发明的数据处理设备也可使用例如 RAS(Rivest Shamir, Adleman; ANSI X9.31))密码翻译，它是一种类似的公共密码系统。

以下说明图 11 中的各个步骤。在步骤 S1 中，设置了下列定义：标号 P 表示特征，a 和 b 表示椭圆曲线的系数(椭圆曲线：$y^2=x^3+ax+b$)，G 表示椭圆曲线上的基点，r 表示 G 的数值， Ks 表示保密密 $0<Ks<r$)。在步骤 S2 中，计算用于消息 M 的散列值以获得 f=Hash(M)。

然后，说明用于用散列函数来确定散列值的方法。散列函数接收作为输入的消息，将其压缩成预定位长度的数据并将压缩后的数据输出为散列值。散列值的特征在于，难以从散列值(输出)预测出输入，当输入给散列函数的数据的一个位有变化时，散列值的多个位就会发生变化，并且，用相同的散列值难以发现不同的输入数据。散列函数可以是与图 7 或其它图所述的相类似的 MD4、MD5 或 SHA-1 或 PES-CBC。在这种情况下，是最终输出值的 MAC(与整体性检查值 ICV 相对应)是散列值。

此后，在步骤 S3 中，生成随机数 u，在步骤 S4 中，基点乘以 u，以获得坐标 V(Xv、Yv)。椭圆曲线上加 2 和乘 2 定义如下：

如果 P=(Xa，Ya)，则 Q=(Xb，Yb)，R=(Xc，Yc)=P+Q。

当 P≠Q(加法)时

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda x(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xb)$

当 P=Q(乘以 2)时

$Xc=\lambda^2-2Xa$

$Yc=\lambda x(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$ ……(1)

这些用于将点 G 乘以 u(尽管计算速度慢，但以下示到了最易于理解的计算方法。计算 G、2×G、4×G。u 是按二进制扩展的，将 $2^I\times G$(通过使 G 乘以 2i 次获得的值)增加给 1 的位(I 表示从 LSB 开始计数的位的位置)。

在步骤 S5 中，计算 c=Xv mod r。在步骤 6 中，判断结果是否为零。如果结果不是零，则在步骤 S7 中计算 d=[(f+cKs)/u] mod r，在步骤 S8 中判断 d 是否为零。如果 d 不是零，则在步骤 S9 中将 c，d)输出为电子签名数据。当假定 r 表示 160 位的长度时，电子签名数据具有 320 位的长度。

如果在步骤 S6 中 c 为 0，则处理过程返回步骤 S3，以重新生成一新的随机数。与此相似，如果在步骤 S8 中 d 为零，处理过程也返回步骤 S3，以重新生成一新的随机数。

(3-3)基于公共密钥密码系统的电子签名验证

以下参照图 12 说明用公共密钥密码系统验证电子签名。在步骤 S11 中，设置以下定义：标号 M 表示消息，标号 p 表示特征，标号 a 和 b 表示椭圆曲线的系数 C 椭圆曲线：$y^2=x^3+ax+b$)，标号 G 表示曲线上的基点，标号 r 表示 G 的数值，标号 G 和 Ks×G 表示公共密钥(0<Ks<r)。在步骤 S12 中，验证电子签名数据 c 和 d 满足 0<c<r 且 0<d<r。如果数据满足这些条件，则在步骤 S13 中，计算用于消息 M 的散列值，以获得 f=Hash(M)。然后，在步骤 S14 中，计算 h=1/d mod r，在步骤 S15 中，计算 h1=fh mod r，h2=ch mod r。

在步骤 S16 中，用已计算出的 h1 和 h2 计算 P=(Xp，Yp)=h1×G+h2.Ks×G。电子签名验证器知道共公密钥 G 和 Ks×G，从而与图 11 中步骤 S4 相类似那样能计算出点在椭圆曲线上的数量乘法。然后，在步骤 S17 中，判断 P 是否是无限远处的点，如果不是，处理过程前进至步骤 S18(实际在步骤 S16 处判断 P 是否是无限远处的点，也就是说，当 P=(X，Y)且 Q=(X，-Y)加到一起时，不可能计算出 λ，以表示 P+Q 是无限远处的点)。在步骤 S18 中，计算 Xp mod r 并与电子签名数据 c 相比较。最后，如果这些值是相等的，所述处理过程前进至步骤 S19，以确定电子签名是正确的。

如果判断出电子签名是正确的，则数据未被篡改，掌握与公共密钥相对应的保密密钥的人业已生成了电子签名。

如果在步骤 S12 签名数据 c 或 d 不满足 0<c<r 或 0<d<r，则处理过程前进至步骤 S20。此外，如果在步骤 S17 中 P 是无限远处的点，则处理过程也前进至步骤 S20。此外，如果在步骤 S18 中 Xp mod r 不等于签名数据，则处理过程前进至步骤 S20。

如果在步骤 S20 中判断出签名是不正确的，这就表示接收到的数据已被篡改或不是由掌握与共公密钥相对应的保密密钥的人所生成的。

(3-4)基于共用密钥密码系统的相互鉴别

以下参照图 13 说明用共用密钥密码系统的相互鉴别。在附图中，共用密钥密码系统是 DES，但也可以使用与前述相类似的任何共用密钥密码系统。在图 13 中，B 首先生成 64 位的随机数 Rb 并将 Rb 及其自己的 ID ID(b)传给 A。在接收到数据时，A 生成新的 64 位随机数 Ra、用密钥 Kab 按 Ra、Rb 和 ID(b)的次序在 DES CBC 模式下对数据加密并将它们返回给 B。依照图 7 所示的 DES CBC 模式处理结构，Ra、Rb 和 ID(b)对应用于 M1、M2 和 M3，并且，在初始值：IV=0 时，输出 E1、E2 和 E3 是加密的文本。

在接收到数据时，B 用密钥 Kab 对接收到的数据解密。为了对接收到的数据解密，首先用密钥 Kab 对加密的文本 E1 进行解密，以便获得随机数 Ra。然后，用密钥 Kab 对加密的文本 E2 进行解密，其结果与 E1 作异或运算，以便获得 Rb。最后，用密钥 Kab 对加密的文本 E3 进行解密，其结果与 E2 作异或运算，以便获得 ID(b)。在这样获得的 Ra、Rb

和 ID(b)中，检查 Rb 和 ID(b)与 B 所传送的那些值的等同性。如果对它们进行了成功的验证，则 B 鉴别了 A。

然后，B 生成在鉴别之后使用的会话密钥(以下称“Kses”)(它是用随机数生成的)。用密钥 Kab 按这样的次序在 DES CBC 模式下对 Rb、Ra 和 Kses 加密并将它们返回给 A。

在接收到数据时，A 用密钥 Kab 对接收到的数据解密。用于对接收到的数据进行解密的方法类似于 B 所执行的方法，所以略去对它的详细说明。在这样获得的 Ra、Rb 和 Kses 中，检查 Rb 和 Kses 与 A 所传送的那些值的等同性。如果对它们进行了成功的验证，则 A 鉴别了 B。在 A 和 B 已相互鉴别之后，将会话密钥 Kses 用作公用密钥，它在鉴别之后用于保密通信。

如果在接收到的数据的验证过程中发现非法性和不等同性，则认为相互鉴别已失败，并中断处理过程。

(3-5)公共密钥证书

以下参照图 14 说明公共密钥证书。公共密钥证书是由公共密钥密码系统的证书管理机构(CA)颁发的。当用户将他或她自己的 ID、公共密钥及其它数据提交给证书管理机构时，管理机构就将诸如自己的 ID 和有效期之类的信息增加给用户提交的数据并还将其签名增加给所述数据，以生成公共密钥证书。

图 14 所示的公共密钥证书包含证书的版本号、由证书管理机构分配给证书用户的证书序号、用于电子签名的算法和参数、证书管理机构的名称、证书的有效期、证书用户的名称(用户 ID)以及证书用户的公共密钥和电子签名。

电子签名是通过将散列函数应用于证书的版本号、由证书管理机构分配给证书用户的证书序号、用于电子签名的算法和参数、证书管理机构的名称、证书的有效期、证书用户的名称(用户 ID)以及证书用户的公共密钥的全部以便生成散列值然后使用该散列值的证书管理机构的保密密钥而生成的数据。例如，用图 11 所述的流程生成电子签名。

证书管理机构颁发图 14 所示的公共密钥证书、更新有效期已到期的公共密钥证书、创建、管理并发布非法用户列表，以便排除有不法行为的用户(以下称为“撤消”)。证书管理还按需生成公共和保密密钥。

另一方面，为了使用上述公共密钥证书，用户用证书管理机构所本身所持有的公共密钥去验证公共密钥证书上的电子签名，在已成功验证电子签名之后，用户从公共密钥证书中取出公共密钥并使用该密钥。因此，所有使用公共密钥证书的用户均持有证书管理机构的共用公共密钥。图 12 说明了用于验证电子管理机构的方法，故略去了对它的详细说明。

(3-6)基于公共密钥密码系统的相互鉴别

以下参照图 15 说明用 160 位椭圆曲线密码翻译进行相互鉴别的方法，所述椭圆曲线密码翻译是公共密钥密码翻译。在附图中，公共密钥密码系统是 ECC，但也可如前所述那样使用任何类似的公共密钥密码系统。此外，密钥长度并不限于 160 位。在图 15 中，B 首先生成 64 位的随机数 Rb 并将 Rb 及其自己的 ID ID(b)传给 A。在接收到数据时，A 生成新的 64 位随机数 Ra 以及小于特征 p 的随机数 Ak。然后，A 将基点 G 乘以 Ak 以便确定 Av=Ak × G、生成用于 Ra、Rb 和 Av(X 和 Y 坐标) 的电子签名 A.Sig 并将这些数据连同 A 的公共密钥证书返回给 B。在这种情况下，由于 Ra 和 Rb 均包含 64 位，且 Av 的 X 和 Y 坐标均包含 160 位，故电子签名总数为 448 位。业已在图 11 中说明了生成电子签名的方法，故略去了对它的详细说明。图 14 中说明了公共密钥证书，故略去了对它的详细说明。

在接收到 A 的公共密钥证书 Ra、Rb 和电子签名 A.Sig 时，B 就验证 A 所传送的 Rb 与 B 所传送的 Rb 是否相匹配。如果判断出它们是相匹配的，则 B 用证书管理机构的公共密钥验证 A 的公共密钥证书中的电子签名并取出 A 的公共密钥。业已参照图 14 说明了公共密钥证书的验证，故略去了对它的详细说明。然后，B 用所获得的 A 的公共密钥去验证电子签名 A.Sig。业在图 12 中说明了验证电子签名的方法，故略去了对它的详细说明。一旦对电子签名进行了成功的验证，则 B 鉴别了 A。

然后，B 生成小于特征 p 的新随机数。此后，B 将基点 G 乘以 Bk 以确定 Bv=Bk × G、生成生成用于 Ra、Rb 和 Bv(X 和 Y 坐标) 的电子签名 A.Sig 并将这些数据连同 B 的公共密钥证书返回给 B。

在接收到 B 的公共密钥证书 Rb、Ra、Rb、Av 和电子签名 B.Sig 时，A 就验证 B 所传送的 Ra 与 A 所传送的 Ra 是否相匹配。如果判断出它们

是相匹配的，则 A 用证书管理机构的公共密钥验证 B 的公共密钥证书中的电子签名并取出 B 的公共密钥。然后，A 用所获得的 B 的公共密钥去验证电子签名 B.Sig。一旦对电子签名进行了成功的验证，则 A 鉴别了 B。

如果 A 和 B 彼此成功地进行鉴别，B 就计算 Bk × Av(由于 Bk 是随机数，但 Av 是椭圆曲线上的点，故椭圆曲线上的点必须进行标量乘法)，并且，B 计算 Ak × Bv，因此，可将这些点的各 X 坐标的低 64 位用作供以后通信中使用的会话密钥(如果共用密钥密码翻译使用 64 位密钥长度的话)。当然，可根据 Y 坐标生成会话密钥，或者，不使用低 64 位。在相互鉴别之后的保密通信中，不仅用会话密钥对所传送的数据加密，而且可将电子签名增加给所传送的数据。

如果在电子签名或接收到的数据的验证过程中发现非法性和不等同性，则认为相互鉴别已失败，并中断处理过程。

(3-7)用椭圆曲线密码翻译的加密过程

以下参照图 16 说明用椭圆曲线密码翻译的加密。在步骤 S21 中，设置了如下定义：标号 Mx 和 Mr 表示消息，标号 p 表示特征，标号 a 和 b 表示椭圆曲线的系数(椭圆曲线：$y^2=x^3+ax+b$)，标号 G 表示曲线上的基点，标号 r 表示 G 的数值，标号 G 和 Ks×G 表示公共密钥(0<Ks<r)。在步骤 S22 中，生成随机数 u，因此，0<u<r。在步骤 S23 中，密钥将公共密钥 Ks×G 乘以 u 而计算出坐标 V。图 11 中的步骤 S4 说明椭圆曲线上的标量乘法，因此略去了对它的说明。在步骤 S24 中，V 的 X 坐标乘以 Mx 然后除以 p，以便确定余数 X0。在步骤 S25 中，V 的 Y 坐标乘以 My 然后除以 p，以便确定余数 Y0。如果消息的长度小于位的数量，则 My 包括一随机数，解密部废弃掉该数。在步骤 S26 中，计算 u×G，在步骤 S27 中，获得加密的文本。

(3-8)用椭圆曲线密码翻译的解密过程

以下参照图 17 说明椭圆曲线密码翻译的解密。在步骤 S31 中，设置了以下定义：标号 u×G，(X0，Y0)表示加密的文本，称号 p 表示特征。称号 a 和 b 表示椭圆曲线的系数(椭圆曲线：$y^2=x^3+ax+b$)，标号 G 表示曲线上的基点，标号 r 表示 G 的数值， 标号 Ks 表示保密密钥(0<Ks<r)。在步骤 S32 中，加密数据(u×G)乘以与保密密钥 Ks 相对定的值，以确定坐标(Xv、yv)。在步骤 S33 中，从加密的文本数据中取

出(X0，Y0)的X坐标并计算X1=X0/Xv mod p。在步骤S34中，取出Y坐标并计算Y1=Y0/Yv mod p。在步骤S35中，将X1确定为Mx，将Y1确定为My，以获得消息。这时，如果My不用于消息，则废弃掉Y1。

通过这种方式，当保密密钥是Ks，公共密钥是G，计算Ks×G，用于加密的密钥和用于解密的密钥可以是不同的。

公共密钥密码翻译的另一个周知实例是RSA，但略去了对它的详细说明(PKCS#1版本2中说明了其细节)。

(3-9)随机数生成过程

以下说明生成随机数的方法。周知的随机数生成方法包括放大热噪音以根据最终A/D输出生成随机数的固有随机数生成方法以及将诸如M序列之类的多个线性电路结合在一起的伪随机数生成方法。还周知有使用诸如DES之类的共用密钥密码翻译的方法。在本例中，说明用DES的伪随机数生成方法(基于ANSI X9.17)。

首先，将从诸如时间之类数据中获得的64位值(就较小的位数而言，较高的位设置成0)限定为D，将用于三重DES的密钥信息限定为Kr，将用于生成随机数的种子限定为S。这样，按下式计算随机数:

I=三重DES(Kr，D)……(2-1)

I=三重DES(Kr，S⊕I)……(2-2)

I=三重DES(Kr，R⊕I)……(2-3)

在这种情况下，三重DES()是这样的函数，它将第一参数用作密码翻译密钥信息并根据三重DES对第二参数的值加密。操作⊕是每64位执行的异或。将最后的值S更新为新种子。

如果连续地生成随机数，则重复等式(2-2)和(2-3)。

业已说明了适用于本发明数据处理设备的多种密码翻译处理过程的方面。以下详细说明本发明数据处理设备中执行的具体过程。

(4)、存储在记录和再现设备中的数据的结构

图18是用于说明图3所示记录和再现设备300的记录和再现设备密码翻译处理部302中内部存储器307内保存的数据内容的图。

如图18所示，内部存储器307存储有以下密钥和数据:

MKake: 记录设备鉴别主密钥，它用于生成在记录和再现设备300与记录设备400之间执行的相互鉴别过程所需的鉴别和密钥交换密钥(以下称为“Kake”)(见图3)。

IVake: 用于记录设备鉴别密钥的初始值。

MKdis: 用于发布密钥的主密钥，所述发布密钥用于生成发布密钥 Kdis。

Ivdis: 发布密钥生成初始值

Kicva: 整体性检查值 A 生成密钥，它用于生成整体性检查值 ICVa。

Kicvb: 整体性检查值 B 生成密钥，它用于生成整体性检查值 ICVb。

Kicvc: 内容整体性检查值生成密钥，它用于生成各内容块的整体性检查值 ICVi(i=1 至 N)。

Kicvt: 总体整体性检查值生成密钥，它用于生成总体整体性检查值 ICVt。

Ksys: 系统签密钥，它用于将共用签名或 ICV 增加给发布系统。

Kdev: 记录和再现设备签名密钥，它随记录和再现设备而变并且由记录和再现设备所使用以便增加签名或 ICV。

IVmem: 用于相互鉴别处理过程的密码翻译处理过程或类似过程的初始值。该值由记录设备所共享。

上述密钥和密钥存储存记录和再现设备密码翻译处理部 302 的内部存储器 307 中。

(5)、存储在记录设备中的数据的结构

图 19 是示出了如何将数据保存在记录和再现设备上的图。在该图中，内部存储器 405 被划分成多个块(本例中为 N)，每个块均存储有以下密钥和数据:

IDmen: 记录设备标识信息，它是记录设备所独有的。

Kake: 鉴别密钥，它用于和记录和再现设备 300 的相互鉴别。

IVmem: 初始值，它用于相互鉴别或类似过程的密码翻译处理过程。

Kstr: 存储密钥，它是用于块信息和其它内容数据的密码翻译密钥。

Kr: 随机数发生密钥

S: 种子。

这些数据均保存在相应的块内。外部存储器 402 保存有多个内容数据(本例中为 M)，外部存储器 402 保存有图 4 所述例如在图 26 或 27 所示的数据。以下说明图 26 与 27 之间结构差异。

(6)、记录和再现设备与记录设备之间的相互鉴别处理过程

(6-1)相互鉴别过程概要

图 20 是示出记录和再现设备 300 与记录设备 400 之间鉴别的过程的流程图。在步骤 S41 中，用户将记录设备 400 插进记录和再现设备 300。但是，如果记录设备 400 能以非接触的方式通信，则不必插入记录设备。

当将记录设备 400 置于记录和再现设备 300 内时，图 3 所示的记录和再现设备 300 中的记录设备检测装置(未示出)就通知控制部 301 记录设备 400 已经安装。然后，在步骤 S42 中，记录和再现设备 300 的控制部 301 通过记录设备控制器 303 将初始化命令传给记录设备 400。在接收到命令时，记录设备 400 使记录设备密码翻译处理部 401 的控制部 403 通过通信部 404 接收命令并在设置有鉴别完成标志的情况下清除该标志。也就是说，设置成未鉴别的状态。

然后，在步骤 S43 中，记录和再现设备 300 的控制部 301 将初始化命令传给记录和再现设备密码翻译处理部 302。这时，控制部还发送记录设备插入端口号。当发送记录设备插入端口号时，即使有多个记录设备 400 与记录和再现设备 300 相连，记录和再现设备 300 也可同时进行与这些记录设备的鉴别并将数据发送给记录设备和接收来自记录设备的数据。

在接收到初始化命令时，如果已设置了与记录设备插入端口号相对应的签别完成标志，则记录和再现设备 300 的记录和再现设备密码翻译处理部 302 使其控制部 306 清除该标志。也就是说，设置成未鉴别的状态。

在步骤 S44 中，记录和再现设备 300 的控制部 301 指定记录设备 400 的记录设备密码翻译处理部 401 所使用的密钥块号。以后将说明密钥块号的细节。在步骤 S45 中，记录和再现设备 300 的控制部 301 读出存储在记录设备 400 的内部存储器 405 内指定密钥块中的记录设备标识信息 IDmem。在步骤 S46 中，记录和再现设备 300 的控制部 301 将记录设备标识信息 IDmem 发送给记录和再现设备密码翻译处理部 302，以便根据记录设备标识信息 IDmem 生成鉴别密钥 Kake。例如按以下方式生成鉴别密钥 Kake:

$$Kake=DES(MKake,\ IDmem \oplus IVake) \cdots\cdots (3)$$

在这种情况下，MKake 表示用于记录设备鉴别密钥的主密钥，所述记录设备鉴别密钥用于生成记录和再现设备 300 与记录设备 400 之间执行的相互鉴别过程所需的鉴别密钥(见图 3)，所述主密钥如上所述存储在记录和再现设备 300 的内部存储器中。此外，IDmem 表示记录设备 400 所独有的记录设备标识信息。再有，IVake 表示用于记录设备鉴别密钥的初始值。此外，在上述等式中，DES()表示这样的函数，它将第一参数用作密码翻译密钥并根据 DES 对第二参数的值加密。操作⊕表示每 64 执行的异或运算。

如果例如应用了图 7 或 8 所示的 DES 结构，则图 7 和 8 所示的消息 M 与记录设备标识信息 IDmem 相对应，密钥 K1 与用于设备鉴别密钥的主密钥 MKake 相对应，初始值 IV 与值 IVake 相对应，所获得的输出是鉴别密钥 Kake。

然后，在步骤 S47 中，执行相互鉴别处理过程和用于生成会话密钥 Kses 的过程。在记录和再现设备密码翻译处理部 302 的加密/解密部 308 与记录设备密码翻译处理部 401 的加密/解密部 406 之间进行相互鉴别，记录和再现设备 300 的控制部 301 在两者之间作调解。

可如以上在图 13 中所述那样进行相互鉴别处理过程。在图 13 所示的结构中，A 和 B 分别对应于记录和再现设备 300 和记录设备 400。首先，记录和再现设备的记录和再现设备密码翻译处理部 302 生成随机数 Rb 并将 Rb 和是其自己的 ID 的记录和再现设备标识信息 IDdev 发送给记录设备 400 的记录设备密码翻译处理部 401。记录和再现设备标识信息 IDdev 是存储在记录和再现设备 300 的存储部中的为再现设备所独有的标识符。记录和再现设备标识信息 IDdev 可记录在记录和再现设备密码翻译处理部 302 的内部存储器中。

在接收到随机数 Rb 和记录和再现设备标识信息 IDdev 时，记录设备 400 的记录设备密码翻译处理部 401 生成新的 64 位随机数 Ra、用鉴别密钥 Kake 按 Ra、Rb 和记录和再现设备标识信息 IDdev 的次序在 DES CBC 模式下对数据加密并将它们返回给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。例如，依照图 7 所示的 DES CBC 模式处理结构，Ra、Rb 和 IDdev 分别对应用于 M1、M2 和 M3，并且，在初始值：IV=IVmem 时，输出 E1、E2 和 E3 是加密的文本。

在接收到加密的文本 E1、E2 和 E3 时，记录和再现设备 300 的记

录和再现设备密码翻译处理部 302 用鉴别密钥 Kake 对接收到的数据解密。为了对接收到的数据解密，首先用密钥 Kake 对加密的文本 E1 进行解密，其结果与 IDmem 作异或运算，以便获得随机数 Ra。然后，用密钥 Kake 对加密的文本 E2 进行解密，其结果与 E1 作异或运算，以便获得 Rb。最后，用密钥 Kake 对加密的文本 E3 进行解密，其结果与 E2 作异或运算，以便获得记录和再现设备标识信息 IDdev。在这样获得的 Ra、Rb 和记录和再现设备标识信息 IDdev 中，检查 Rb 和记录和再现设备标识信息 IDdev 与记录和再现设备 300 所传送的那些值的等同性。如果对它们进行了成功的验证，则记录和再现设备 300 的记录和再现设备密码翻译处理部 302 鉴别了记录设备 400。

然后，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 生成在鉴别之后使用的会话密钥(以下称“Kses”)(它是用随机数生成的)。用密钥 Kake 按这样的次序在 DES CBC 模式下对 Rb、Ra 和 Kses 加密并将它们返回给记录设备 400 的记录设备密码翻译处理部 401。

在接收到数据时，记录设备 400 的记录设备密码翻译处理部 401 用密钥 Kake 对接收到的数据解密。用于对接收到的数据进行解密的方法类似于记录和再现设备 300 的记录和再现设备密码翻译处理部 302 所执行的方法，所以略去对它的详细说明。在这样获得的 Ra、Rb 和 Kses 中，检查 Rb 和 Kses 与记录设备 400 所传送的那些值的等同性。如果对它们进行了成功的验证，则记录设备的记录设备密码翻译处理部 401 鉴别了记录和再现设备 300。在这些设备已相互鉴别之后，将会话密钥 Kses 用作公用密钥，它在鉴别之后用于保密通信。

如果在接收到的数据的验证过程中发现非法性和不等同性，则认为相互鉴别已失败，并中断处理过程。

如果成功地进行相互鉴别，所述处理过程从步骤 S48 前进至步骤 S49，在步骤 S49 中，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 保存会话密钥 Kses，并设置鉴别完成标志，以表示完成了相互鉴别。此外，如果相互鉴别失败，则处理过程前进至步骤 S50，废弃会话密钥 Kses 并清除鉴别完成标志。如果所述标志已被清除，则不一定需要清除过程。

如果从记录插入端口除去记录设备 400，则记录和再现设备 300 中的记录设备检测装置就通知记录和再现设备 300 的控制部 301 已除去

了记录设备 400。对此进行响应，记录和再现设备 300 的控制部 301 命令记录和再现设备 300 的记录和再现设备密码翻译处理部 302 去清除与记录设备插入端口号相对应的鉴别完成标志。对此进行响应，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 清除与记录设备插入端口号相对应的鉴别完成标志。

业已说明了按图 13 所示过程进行相互鉴别处理的实例，但是，本发明并不局限于鉴别过程的上述实例，而是可以根据图 15 中的相互鉴别实例来进行处理。另外，在图 13 所述的过程中，图 13 中的 A 可设定为记录和再现设备 300，B 可设定为记录设备 400，可将 B：记录设备 400 首先发送给 A：记录和再现设备 300 的 ID 设定为记录设备中的密钥块内的记录设备标识信息。可将多种处理过程应用于本发明中执行的鉴别处理过程，并且，本发明并不局限于上述鉴别过程。

(6-2)在相互鉴别过程中切换密钥块

本发明数据处理设备中的相互鉴别过程的部分特征在于，通过在记录设备 400 一方配置多个密钥块(例如为 N)并使记录和再现设备 300 指定其中之一(图 20 的流程中的步骤 S44)而执行鉴别过程。如前在图 19 中所述，配置在记录设备 400 的密码翻译处理部 401 中的内部存储器 405 里形成有多个密钥块，它们存储有诸如密钥数据和 ID 信息之类的不同数据。在图 19 中的记录设备 400 的多个密钥块之一上执行记录和再现设备 300 与记录整体性检查值 400 之间如图 20 所述那样执行的相互鉴别过程。

用于执行记录介质与再现设备之间的相互鉴别过程的通常结构一般使用用于相互鉴别的共用鉴别密钥。因此，当鉴别密钥就各产品目的地(国家)或产品而言要加以改变时，必须在记录和再现设备及记录设备上改变用于这两种设备的鉴别处理过程所需的密钥数据。因此，存储在新售出的记录和再现设备内的鉴别过程所需的密钥数据不与存储在先前售出的记录和再现设备内的鉴别过程所需的密钥数据相对应，所以，新的记录和再现设备不能访问旧版本的记录设备。相反，在新版记录设备与旧版记录和再现设备之间的关系方面也有类似的情况。

在本发明的数据处理设备中，密钥块作为图 19 所示的多个不同密钥集合存储在记录设备 400 内。记录和再现设备具有要应用于鉴别过

程的密钥块，即例如就各产品目的地(国家)、产品、设备类型、版本或应用而言具有指定的密钥块集合。这种集合信息存储在记录和再现设备的存储部内例如存储在图 3 的内部存储器内或记录和再现设备 300 的其它存储部件内，并且在鉴别过程中由图 3 中的控制部 301 所访问，以便根据这种集合信息指定密钥块。

用于记录和再现设备 300 的内部存储器 307 中的记录设备鉴别密钥的主密钥 Mkake 是根据用于指定密钥块的设置集而设置的，并且仅对应于该指定的密钥块，它不会与指定块之外的任何密钥块形成相互鉴别。

如图 19 所示，记录设备 400 的内部存储器 405 具有 N 个密钥块(1 至 N)集合，每个集合均存储有记录设备标识信息、鉴别密钥、初始值、存储密钥、随机数生成密钥以及种子，每个密钥块均至少将鉴别密钥数据存储为随密钥块而变的数据。

通过这种方式，记录设备 400 中的密钥块的密钥数据结构随密钥块而变。因此，例如，可将某一记录和再现设备 A 用用于存储在内部存储器中的记录设备鉴别密钥的主密钥 MKake 按其执行鉴别过程的密钥块设置为密钥块一号，并且，将具有不同规格的记录和再现设备 B 按其执行鉴别过程的密钥块设置为另一密钥块例如密钥块二号。

尽管以下将作详细说明，但是，当内容存储在记录设备 400 的外部存储器 402 内时，存储在各密钥块内的存储密钥 Kstr 用于对内容进行加密和存储。具体地说，存储密钥用于对内容密钥进行加密，而密钥密钥则用于对内容块进行加密。

如图 19 所示，存储密钥配置成随密钥块而变的密钥。因此，可防止存储在记录设备的存储器中的内容被两个不同记录和再现设备设置集所共享去指定不同的密钥块。也就是说，不同设置的记录和再现设备仅能使用存储在与其设置相兼容的记录设备中的内容。

可按上述方式形成为各密钥块所共用的数据，同时，例如，仅有鉴别密钥数据和存储密钥数据可随密钥块而变。

在记录设备中配置有包括多个不同密钥数据的密钥块的具体实例中，例如，为不同类型的记录和再现设备 300(安装类型、便携式类型等)设置要加以指定的不同密钥块号，或者，为不同的应用设置不同的指定密钥块。此外，可为不同的地区设置不同的密钥块，例如，为日

本出售的记录和再现设备指定密钥块一号，为美国出售的记录和再现设备指定密钥块二号。利用这种结构，即使诸如存储卡之类在记录设备从美国传至日本或者相反，也不能在有不同密钥设置的记录和再现设备中使用在不同地区使用的并存储在有不同存储密钥的各记录设备内的内容，从而，能防止非法和无序地发布存储在存储内的内容。具体地说，这就有助于排除在两个不同的国家相互使用用不同存储密钥 Kstr 进行加密的内容密钥 Kcon 的情况。

而且，图 19 中所示的记录设备 400 的内部存储器 405 中的密钥块 1 至 N 中的至少一个例如第 N 号密钥块可被任何记录和再现设备 300 所共享。

例如，当密钥块第 N 号和用于能进行鉴别的记录设备鉴别密钥的主密钥 MKake 存储在所有设备中时，可在与记录和再现设备 300、应用的类型或目的地国家无关的情况下发布内容。例如，可在任何设备中使用存储在存储卡中的加密内容，所述存储卡带有存储在密钥块第 N 号内的存储密钥。例如，可通过用共享密钥块中的存储密钥对数据进行加密、将它们存储到存储卡内并将存储卡设置到例如存储有用于记录设备鉴别密钥的主密钥 MKake 的便携式声音再现设备，从而从存储卡中对音乐数据或类似数据进行解密和再现，所述记录设备鉴别密钥也是共享的。

图 21 示出了本发明数据处理设备的用法的实例，它带有多个密钥块。记录和再现设备 2101 是在日本出售的产品并且具有能与记录设备中密钥块一号和四号进行鉴别处理的主密钥。记录和再现设备 2102 是在美国出售的产品并且具有能与记录设备中密钥块二号和四号进行鉴别处理的主密钥。记录和再现设备 2103 是在欧洲出售的产品并且具有能与记录设备中密钥块三号和四号进行鉴别处理的主密钥。

例如，记录和再现设备 2101 与记录设备 2104 中密钥块 1 或 4 进行鉴别，以便将通过存储在密钥块中的存储密钥加以加密的内容存储到外部存储器内。记录和再现设备 2102 与记录设备 2105 中密钥块 2 或 4 进行鉴别，以便将通过存储在密钥块中的存储密钥加以加密的内容存储到外部存储器内。记录和再现设备 2103 与记录设备 2106 中密钥块 3 或 4 进行鉴别，以便将通过存储在密钥块中的存储密钥加以加密的内容存储到外部存储器内。然后，如果记录设备 A2104 安装在记

录和再现设备 2102 或 2103 内，则用密钥块 1 中的存储密钥加以加密的内容不能使用，因为，在记录和再现设备 2102 或 2103 与密钥块 1 之间不能形成鉴别。另一方面，用密钥块 4 中的存储密钥加以加密的内容能够使用，因为，在记录和再现设备 2102 或 2103 与密钥块 4 之间能形成鉴别。

如上所述，在本发明的数据处理设备中，包括多个不同密钥集合的密钥块配置在记录设备内，而记录和再现设备则存储有主密钥，以便能进行用于特定密钥块的鉴别，从而能根据不同的使用形式设置对内容使用的限制。

而且，可在一个记录和再现设备中指定多个密钥块例如 1 至 k，而在另一个记录和再现设备中指定多个密钥块 p 和 q。此外，可提供多个可共享的密钥块。

(7)、用于从记录和再现设备中下载至记录设备的过程

以下说明本发明数据处理设备中用于从记录和再现设备 300 中将内容下载至记录设备 400 的外部存储器过程。

图 22 是用于说明从记录和再现设备 300 中将内容下载至记录设备 400 的流程。在该图中，假定已完成了记录和再现设备 300 与记录设备 400 之间的上述相互鉴别过程。

在步骤 S51 中，记录和再现设备 300 的控制部 301 用读取部 304 从存储有内容的介质 500 中读出有预定格式的数据或者用通信部 305 依照预定格式接收来自通信装置 600 的数据。然后，记录和再现设备 300 的控制部 301 将数据的头标部(见图 4)传给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。

在步骤 S52 中，业已在步骤 S51 中接收了头标的记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整体性检查值 A。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥并将内容 ID 和使用策略用作消息的情况下按图 7 所述的 ICV 计算方法来计算整体性检查值 A，如图 23 所示。初始值可以是 IV=0 或者可以是整体性检查值 A 生成初始值，它存储在记录和再现设备密码翻译处理部 302 的内部存储器 307 中。最后，存储在头标中的整体性检查值 A 和检查值 ICVa 一起作比较，如果它们相等，则处理

过程前进至步骤 S53。

如前在图 4 中所述，检查值 A、ICVa 用于验证内容 ID 和使用策略尚未被篡改。如果在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥并将内容 ID 和使用策略用作消息的情况下按图 7 所述 ICV 计算方法计算出的整体性检查值 A 等于存储在头标中的检查值 ICVa，则可判断出内容 ID 和使用策略未被篡改。

然后，在步骤 S53 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 生成发布密钥 Kdis。例如按如下方式生成发布密钥 Kdis:

Kdis=DES(MKdis，内容 ID Φ IVdis)……(4)

在这种情况下，MKdis 表示用于发布密钥的主密钥，所述发布密钥用于生成发布密钥 Kdis，所述主密钥如上所述存储在记录和再现设备 300 的内部存储器中。此外，内容 ID 是内容数据的头标部的标识信息，IVdis 表示发布密钥的初始值。再有，在上述等式中，DES()表示这样的函数，它将第一参数用作密码翻译密钥并对第二参数的值加密。操作 Φ 表示每 64 执行的异或运算。

在步骤 S54 中，记录和再现设备密码翻译处理部 302 的控制部 306 用记录和再现设备密码翻译处理部 302 的加密/解密部 308 并用在步骤 S53 中生成的发布密钥 Kdis 对块信息表密钥 Kbit 和内容密钥 Knon 进行解密(见图 4)，所述块信息表密钥 Kbit 和内容密钥 Knon 存储在通过读取部 304 从介质 500 中获得或者通过通信部 305 接收自通信装置 600 的数据的头标部内。如图 4 所示，块信息表密钥 Kbit 和内容密钥 Knon 事先用诸如 DVD 或 CD 之类的介质上或诸如因特网之类通信路径上的发布密钥 Kdis 来加密。

在步骤 S55 中，记录和再现设备密码翻译处理部 302 的控制部 306 用记录和再现设备密码翻译处理部 302 的加密/解密部 308 借助在步骤 S54 中解密的块信息表密钥 Kbit 对块信息表(BIT) 进行解密。如图 4 所示的块信息表(BIT)事先用诸如 DVD 或 CD 之类的介质上或诸如因特网之类通信路径上的块信息表密钥 Kbit 来加密。

再有，在步骤 S56 中，记录和再现设备密码翻译处理部 302 的控制部 306 将块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)分成 8

字节的段，它们全都作异或运算(也可以使用诸如加或减之类的任何操作)。然后，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整体性检查值 B(ICVb)。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥而生成整体性检查值 B，以便根据 DES 对先前计算出的异或值进行解密，图 24 所示。最后，在头标中的整体性检查值 B 和检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S57。

如前在图 4 中所述，检查值 B、ICVb 用于块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)尚未被篡改。如果通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥、将块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)分成 8 字节的段、对这些数据作异或运算并根据 DES 对作了异或运算的数据进行加密而生成的的整体性检查值 B 等于存储在头标中的检查值 ICVb，则可判断出块信息表密钥 Kbit、内容密钥 Kcon 和块信息表未被篡改。

在步骤 S57 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算中间整体性检查值。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的总体整体性检查值生成密钥 Kicvt 用作密钥并将整体性检查值 A 和 B 以及所有保存的内容整体性检查值用作消息的情况下按图 7 所述的 ICV 计算方法来计算上述中间值。初始值可以是 IV=0 或者可以使用总体整体性检查值生成初始值，它存储在记录和再现设备密码翻译处理部 302 的内部存储器 307 中。此外，所生成的中间整体性检查值按需存储在记录和再现设备 300 的记录和再现设备密码翻译处理部 302 内。

通过将整体性检查值 A 和 B 以及所有保存的内容整体性检查值用作消息而生成中间整体性检查值，通过将各整体性检查值所验证的数据与中间整体性检查值相比较，可以验证这些数据。但是，在本实施例中，可根据中间整体性检查值独立地生成多个不同的整体性检查值即总体整体性检查值 ICVt 和为记录和再现设备 300 所独有的检查值 ICVdev，因此，可有区别地执行用于验证没有篡改的过程和用于标识

仅被各记录和再现设备 300 在下载过程之后占用的被占用数据的验证过程，可就整个系统的共享数据而言执行所述用于验证没有篡改的过程。

记录和再现设备密码翻译处理部 302 的控制部 306 促使记录和再现设备密码翻译处理部 302 的加密/解密部 308 去计算总体整体性检查值 ICVt。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的系统签名密钥 Ksys 用作密钥而生成总体整体性检查值 ICVt，以便根据 DES 对中整体性检查值进行解密。最后，总体整体性检查值 AICVt 和在步骤 S51 中存储在头标中的 ICVt 一起作比较，如果它们相等，则处理过程前进至步骤 S58。所述系统签名密钥 Ksys 为多个记录和再现设备所共用，也就是说，整个系统执行记录和再现某些数据的处理过程。

如前在图 4 中所述，总体整体性检查值 ICVt 用于验证所有整体性检查值 ICVa 和 ICVb 以及用于各内容块的整体性检查值尚未被篡改。如果上述过程生成的总体整体性检查值等于存储在头标中的整体性检查值 ICVt，则可判断出所有整体性检查值 ICVa 和 ICVb 以及用于各内容块的整体性检查值未被篡改。

然后，在步骤 S58 中，记录和再现设备 300 的控制部 301 从块信息表(BIT)中取出内容块信息并检查是否要验证任何的内容块。如果要验证任一内容块，则内容整体性检查值已被存储在头标的块信息内。

如果要验证任一内容块，则控制部 301 通过用记录和再现设备 300 的读取部 304 从介质 500 中读出内容块或者通过记录和再现设备 300 的通信部 305 读出接收自通信装置 600 的内容块，并将内容块发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。在接收到内容块时，记录和再现设备 300 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算内容中间值。

通过用在步骤 S54 中解密的内容密钥 Kcon 生成内容中间值，以便在 DES CBC 模式下对输入内容块进行解密，从而将最终的数据分成 8 字节的段并对所有的这些段进行异或运算(也可以使用诸如加或减之类的任何操作)。

然后，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算内容整体性检

查值。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的内容整体性检查值生成密钥 Kicvc 用作密钥而生成内容整体性检查值，以便根据 DES 对内容中间值进行解密。记录和再现设备 300 的控制部 306 将这一内容整体性检查值与在步骤 S51 中接收自记录和再现设备 300 的控制部 301 的内容块中的 ICV 作比较，并将结果传给记录和再现设备 300 的控制部 301。在接收到上述结果且在已成功验证的情况下，记录和再现设备 300 的控制部 301 取出下一个要加以验证的内容块并使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 验证该内容块。重复相类似的验证过程，直至验证了所有的内容块。初始值可以是 IV=0，或者，如果头标生成一方使用了同样的设置，则可以使用内容整体性检查值生成初始值 IVc，它存储在记录和再现设备密码翻译处理部 302 的内部存储器 307 中。此外，所有的经检查的内容整体性检查值均保存在记录和再现设备 300 的记录和再现设备密码翻译处理部 302 内。再有，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 监视验证内容块的次序，以便在次序不对的情况下或者在验证同一内容块两次或多次的情况下认为鉴别失败。如果成功地验证了所有的内容块，则处理过程前进至步骤 S59。

然后，在步骤 S59 中，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 通过使用在相互鉴别过程中可共享的会话密钥 Kses 对在步骤 S54 中解密的块信息表密钥 Kbit 和内容密钥进行加密。记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读取块信息表密钥 Kbit 和内容密钥 Kcon，块信息表密钥 Kbit 和内容密钥 Kcon 是用会话密钥 Kses 来解密的。控制部 301 将这些数据通过记录和再现设备 300 的记录设备控制器 303 传给记录设备 400。

在步骤 S60 中，在接收到传送自记录和再现设备 300 的块信息表密钥 Kbit 和内容密钥 Kcon 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用在相互鉴别过程中可共享的会话密钥 Kses 对接收到的数据进行解密并用存储在记录设备密码翻译处理部 401 的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对解密的数据重新加密。最后，记录和再现设备 300 的控制部 301 通过记录

和再现设备 300 的记录设备控制器 303 从记录设备 400 中读出块信息表密钥 Kbit 和内容密钥 Kcon，块信息表密钥 Kbit 和内容密钥 Kcon 是用存储密钥 Kstr 来重新加密的。它们可用用发布密钥 Kdis 加以加密的块信息表密钥 Kbit 和内容密钥 Kcon 来替换。

在步骤 S61 中，记录和再现设备 300 的控制部 301 从数据的头标部内的使用策略中取出本地化字段，以判断下载的内容是仅用于这一记录和再现设备 300(在这种情况下，将本地化字段置成 1)还是也可由其它相类似记录和再现设备 300 所使用(在这种情况下，将本地化字段置成 0)。如果判断的结果显示出本地化字段置成 1，则处理过程前进至步骤 S62。

在步骤 S62 中，记录和再现设备 300 的控制部 301 使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 计算记录和再现设备所独有的整体性检查值。通过通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的记录和再现设备签名密钥 Kdev 用作密钥而生成记录和再现设备所独有的整体性检查值，以便根据 DES 对中间整体性检查值进行解密。在步骤 S58 中保存上述中间整体性检查值。计算出的为记录和再现设备所独有的整体性检查值 ICVdev 可代替总体整体性检查值。

如上所述，系统签名密钥 Ksys 用于将共用签名或 ICV 附加给发布系统，并且，记录和再现设备签名密钥 Kdev 随记录和再现设备而变并且可由记录和再现设备所使用，以便附加签名或 ICV。也就是说，用系统签名密钥 Ksys 签署的数据可由具有同样系统签名密钥的系统(记录和再现设备)来成功地检查，也就是说，这种数据具有同样的总体整体性检查值，从而能得以共享。但是，如果用记录和再现设备签名密钥 kdev 来签署数据，由于这种签名密钥为记录和再现设备所独有，所以，即便将记录设备插进另一个记录和再现设备中之后试图再现用记录和再现设备签名密钥 Kdev 签署的数据即在签署之后存储在记录设备中的数据，也不能再现这些数据，也就是说，会因不相等的为记录和再现设备所独有的整体性检查值 ICVdev 而出现错误。

因此，在本发明的数据处理设备中，设置本地化字段能将内容任意地设置在整个系统内共享或仅由特定的记录和再现设备所使用。

在步骤 S63 中，记录和再现设备 300 的控制部 301 将内容存储到

记录设备 400 的外部存储器 402 内。

图 26 是示出了如何在本地化字段置成 0 的情况下将内容存储在记录设备中的图。图 27 是示出了如何在本地化字段置成 1 的情况下将内容存储在记录设备中的图。图 26 与 4 的不同仅在于是用发布密钥 Kdis 还是用存储密钥 Kstr 对内容块信息密钥 Kbit 和内容密钥 Kcon 进行加密。图 26 与 27 的不同在于，在图 26 中，用系统签名密钥 Ksys 对根据中间整体性检查值计算出的整体性检查值进行加密，而在图 27 中，则是为记录和再现设备所独有的记录和再现设备签名密钥 Kdev 对上述整体性检查值进行加密。

在图 22 的流程中，如果在步骤 S52 中对整体性检查值 A 的验证失败，如果在步骤 S56 中对整体性检查值 B 的验证失败，如果在步骤 S57 中对总体整体性检查值 ICVt 的验证失败，或者，如果在步骤 S58 中对内容块内容整体性检查值的验证失败，那么，处理过程就前进至步骤 S64，以提供预定的错误显示。

此外，如果在步骤 S61 中本地化字段置成 0，则处理过程跳过步骤 S62 前进至 S63。

(8)记录和再现设备所执行的用于再现存储在记录设备内的信息的过程

以下说明记录和再现设备 300 所执行的用于再现存储在记录设备 400 的外部存储器 402 内的内容信息的过程。

图 28 是用于说明记录和再现设备 300 所执行的用于从记录设备 400 中读出内容并使用该内容的流程图。在图 28 中，假定记录和再现设备 300 与记录设备 400 之间已完成相互鉴别。

在步骤 S71 中，记录和再现设备 300 的控制部 301 用记录设备控制器 303 从记录设备 400 的外部存储器 402 中读出内容。然后，记录和再现设备 300 的控制部 301 将数据的头标传给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。步骤 S72 与“(7)用于从记录和再现设备中下载至记录设备的过程”中所述的步骤 S52 相类似，在这一步骤中，业已接收了头标的记录和再现设备密码翻译处理部 302 的控制部 306 可以使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整体性检查值 A。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥

并将内容 ID 和使用策略用作消息的情况下，按图 7 所述的 ICV 计算方法来计算整体性检查值 A，如先前图 23 所示。

如前所述，检查值 A、ICVa 用于验证内容 ID 和使用策略未被篡改。如果在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥并将内容 ID 和使用策略用作消息的情况下按图 7 所述 ICV 计算方法计算出的整体性检查值 A 等于存储在头标中的检查值 ICVa，则可判断出存储在记录设备 400 中的内容 ID 和使用策略未被篡改。

在步骤 S73 中，记录和再现设备 300 的控制部 301 从读出的头标部中读出块信息表密钥 Kbit 和内容密钥 Knon，然后通过记录和再现设备 300 的记录设备控制器 303 将它们传给记录设备 400。在接收到从记录和再现设备 300 传送的块信息表密钥 Kbit 和内容密钥 Knon 时，记录设备 400 使记录设备密码翻译处理部 401 的加密/解密部 406 用存储在记录设备密码翻译处理部 401 的内部存储器 405 中的为记录的所独用的存储密钥 Kstr 对接收到的数据进行解密，然后用在相互鉴别过程可共享的会话密钥 Kses 对解密的数据进行重新加密。此后，记录和再现设备 300 的控制部 301 通过记录和再现设备 300 的记录设备控制器 303 从记录设备 400 中读出块信息表密钥 Kbit 和内容密钥 Knon，所述块信息密钥 Kbit 和内容密钥 Knon 是用来自记录设备 400 的会话密钥 Kses 来重新加密的。

在步骤 S74 中，记录和再现设备 300 的控制部 301 将接收到的块信息密钥 Kbit 和内容密钥 Kcon 传给记录和再现设备 300 的记录和再现设备密码翻译处理部 302，所述块信息密钥 Kbit 和内容密钥 Knon 是用会话密钥 Kses 来重新加密的。

在接收到用会话密钥 Kses 来重新加密的块信息密钥 Kbit 和内容密钥 Knon 时，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 利用在相互鉴别过程可共享的会话密钥 Kses 对会话密钥 Kses 加以加密的块信息密钥 Kbit 和内容密钥 Knon 进行解密。然后，记录和再现设备密码翻译处理部 302 使加密/解密部 308 用解密的块信息表密钥 Kbit 对在步骤 S71 中接收到的块信息表进行解密。

记录和再现设备 300 的记录和再现设备密码翻译处理部 302 用在

步骤 S71 中接收到的值来代替解密的块信息表密钥 Kbit、内容密钥 Kcon 和块信息表 BIT，以便保存。此外，记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读出解密的块信息表 BIT。

步骤 S75 与“(7)用于从记录和再现设备中下载至记录设备的过程”中所述的步骤 S56 相类似。记录和再现设备密码翻译处理部 302 的控制部 306 将从记录设备 400 中读出的块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)分成 8 字节的段，然后对它们全都作异或运算。记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整体性检查值 B(ICVb)。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥而生成整体性检查值 B，以便根据 DES 对先前计算出的经异或运算的值进行解密，如先前图 24 所示。最后，检查值 B 和头标中的检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S76。

如前所述，检查值 B、ICVb 用于验证块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)未被篡改。如果通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥、将从记录设备 400 中读出的块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)分成 8 字节的段、对这些数据作异或运算并根据 DES 对作了异或运算的数据进行加密而生成的整体性检查值 B 等于存储在头标中的检查值 ICVb，则可判断出块信息表密钥 Kbit、内容密钥 Kcon 和块信息表未被篡改。

在步骤 S76 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算中间整体性检查值。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的总体整体性检查值生成密钥 Kicvt 用作密钥并将整体性检查值 A 和 B 以及所有保存的内容整体性检查值用作消息的情况下按图 7 所述的 ICV 计算方法来计算上述中间值。初始值可以是 IV=0 或者可以使用总体整体性检查值生成初始值 IVt，它存储在记录和再现设备密码翻译处理部 302 的内部存储器 307 中。此外，所生成的中间整体性检查值按需存储在记录和再现设备 300 的记录和再现设备密码翻译

处理部 302 内。

然后，在步骤 S77 中，记录和再现设备 300 的控制部 301 从包含在从记录设备 400 的外部存储器 402 内读出的数据的头标部内的使用策略中取出本地化字段，以判断下载的内容是仅用于这一记录和再现设备 300(在这种情况下，将本地化字段置成 1)还是也可由其它相类似记录和再现设备 300 所使用(在这种情况下，将本地化字段置成 0)。如果判断的结果显示出本地化字段置成 1，也就是说，设置成了下载的内容仅用于这一记录和再现设备 300，则处理过程前进至步骤 S80。如果本地化字段置成 0，也就是说，设置成了下载的内容也可由其它相类似记录和再现设备 300 所使用，则处理过程前进至步骤 S78。步骤 77 由密码翻译处理部 302 来处理。

在步骤 78 中，按与“(7)用于从记录和再现设备中下载至记录设备的过程”中所述的步骤 S58 相同的方式计算总体整体性检查值 ICVt。也就是说，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算总体整体性检查值 ICVt。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的系统签名密钥 Ksys 用作密钥而生成总体整体性检查值 ICVt，以便根据 DES 对中间值进行加密，如先前图 25 所示。

处理过程前进至 S79，以便将步骤 78 中生成的总体整体性检查值 ICVt 与步骤 S71 中存储在头标中的 ICVt。如果这些值相等，则处理过程前进至步骤 S82。

如前所述，总体整体性检查值 ICVt 用于验证整体性检查值 ICVa 和 ICVb 以及所有的内容块整体性检查值未被篡改。因此，如果通过上述过程生成的总体整体性检查值等于存储在头标中的检查值 ICVt，则可判断出在存储器于记录设备 400 中的数据内整体性检查值 ICVa 和 ICVb 以及所有的内容块整体性检查值未被篡改。

如果步骤 S77 中的判断结果显示出本地化字段设置下载的内容仅可用于这一记录和再现设备 300，也就是说，该字段置成 1，则处理过程前进至步骤 S80。

在步骤 S80 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整体性检查值 ICVdev。通过将存储在记录和再现设备密码翻译处理部 302 的

内部存储 307 中的为记录和再现设备所独有的记录和再现设备签名密钥 Kdev 用作密钥而如图 25 所示那样生成记录和再现设备所独有的整体性检查值 ICVdev，以便根据 DES 对中整体性检查值进行解密。所述中间整体性检查值是在步骤 S58 中保存的。在步骤 S81 中，将在步骤 S80 中计算出的为记录和再现设备所独有的检查值 ICVdev 和在步骤 S71 中存储的 ICVdev 一起作比较，如果它们相等，则处理过程前进至步骤 S82。

因此，用相同系统签名密钥 Ksys 签署的数据可由具有同样系统签名密钥的系统(记录和再现设备)来成功地检查，也就是说，这种数据具有同样的总体整体性检查值 ICVt，从而能得以共享。但是，如果用记录和再现设备签名密钥 kdev 来签署数据，由于这种签名密钥为记录和再现设备所独有，所以，即便将记录设备插进另一个记录和再现设备中之后试图再现用记录和再现设备签名密钥 Kdev 签署的数据（即在签署之后存储在记录设备中的数据），也不能再现这些数据，也就是说，会为记录和再现设备所独有的整体性检查值 ICVdev 中的不匹配而出现错误。因此，设置本地化字段能将内容任意地设置在整个系统内共享或仅由特定的记录和再现设备所使用。

在步骤 S82 中，记录和再现设备 300 的控制部 301 从在步骤 S74 中读出的块信息表(BIT)内取出内容块信息并检查是否要加密任何的内容块。如果要加密任一内容块，则控制部 301 通过记录和再现设备 300 的读取设备控制器 303 从记录设备 400 的外部存储器 402 中读出这一内容块，然后将内容块发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。在接收到内容块时，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 对内容解密，而如果内容块要加以验证，则使加密/解密部 308 在步骤 S83 中计算内容整体性检查值。

步骤 S83 与与 “(7)用于从记录和再现设备中下载至记录设备的过程”中所述的步骤 S58 相类似。记录和再现设备 300 的控制部 301 从块信息表(BIT)中取出内容块信息并根据所存储的内容整体性检查值判断是否要验证任何的内容块。如果要验证任一内容块，则控制部 301 从记录设备 400 的外部存储器 402 中接收内容块并将其传给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。在接收到内容块

时，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算内容中间值。

通过用步骤 S74 中解密的内容密钥 Kcon 来生成内容中间值，以便在 DES CBC 模式下对输入内容块进行解密，从而将最终的数据分成 8 字节的段并对所有的段作异或运算。

然后，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算内容整体性检查值。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的内容整体性检查值生成密钥 Kicvc 用作密钥而生成内容整体性检查值，以便根据 DES 对内容中间值进行解密。记录和再现设备 300 的控制部 306 将这一内容整体性检查值与在步骤 S71 中接收自记录和再现设备 300 的控制部 301 的内容块中的 ICV 作比较，并将结果传给记录和再现设备 300 的控制部 301。在接收到上述结果且在已成功验证的情况下，记录和再现设备 300 的控制部 301 取出下一个要加以验证的内容块并使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 验证该内容块。重复相类似的验证过程，直至验证了所有的内容块。初始值可以是 IV=0，或者，可以使用内容整体性检查值生成初始值 IVc，它存储在记录和再现设备密码翻译处理部 302 的内部存储器 307 中。此外，所有的经检查的内容整体性检查值均保存在记录和再现设备 300 的记录和再现设备密码翻译处理部 302 内。再有，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 监视验证内容块的次序，以便在次序不对的情况下或者在验证同一内容块两次或多次的情况下认为鉴别失败。

记录和再现设备 300 的控制部 301 接收内容整体性检查值的比较结果(如果没有内容块要加以验证，则所有的比较结果都是成功的)，并且，如果验证已经成功，则控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中取出解密的内容。然后，控制部 301 取出下一个要加以验证的内容块并使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 对该内容块解密。重复相类似的验证过程，直至对所有的内容块进行了解密。

在步骤 83 中，如果记录和再现设备 300 的记录和再现设备密码翻译处理部 302 在验证过程之后判断出内容整体性检查值不相等，则认

为验证失败并阻止对其余内容进行解密。此外，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 监视对内容块解密的次序，以便在次序不对的情况下或者在对同一内容块解密两次或多次的情况下认为解密失败。

如果在步骤 S72 中整体性检查值 A 的验证已经失败，如果在步骤 S75 中整体性检查值 B 的验证已经失败，如果在步骤 S79 中总体整体性检查值 ICVt 的验证已经失败，如果在步骤 S81 中记录和再现设备所独有的整体性检查值 ICVdev 的验证已经失败，或者，如果在步骤 S81 中内容块内容整体性检查值的验证已经失败，那么，处理过程就前进至步骤 S84，以提供预定的错误显示。

如上所述，不仅在下载或使用内容时可对重要数据进行加密、取消或作篡改检查，而且即便是在将记录介质上的数据简单地拷贝至另一记录介质上，也可防止不正确地对内容进行解密，因为，用于对块信息表 BIT 解密的块信息表密钥和用于对内容进行解密的内容密钥 Kcon 是与记录介质所独有的存储密钥 Kstr 存在一起的。具体地说，例如，在图 28 的步骤 S74 中，另一记录设备不能正确地对数据解密，因为，每个记录设备均对用不同存储密钥 Kstr 加密的数据进行解密。

(9)相互鉴别之后的密钥交换过程

本发明的数据处理设备的部分特征在于，仅在记录和再现设备 300 与记录设备 400 之间的上述相互鉴别过程之后才能使用记录设备 400，并且，记录设备的使用形式是有限的。

例如，为了防止用户生产诸如存储卡之类其中通过非法拷贝或类似行为而存储有内容的记录设备并将这种记录设备在记录和再现设备中使用，在记录和再现设备 300 与记录设备 400 之间进行相互鉴别，并且，只有在它们相互鉴别了的情况下才能在记录和再现设备 300 与记录设备 400 之则传递(加密的)内容。

为了获得上述限制过程，依照本发明的数据处理设备，根据预定命令串执行记录设备 400 的密码翻译处理部 401 中的所有过程。也就是说，记录设备具有这样的命令过程结构，它根据命令号从寄存器中获得命令。图 29 是用于说明记录设备的命令过程结构的图。

如图 29 所示，在具有记录和再现设备密码翻译处理部 302 的记录和再现设备 300 与具有记录设备加密处理部 401 的记录设备 400 之间，

命令号(No.)在记录和再现设备300的控制部301的控制下从记录设备控制器303输出给记录设备400的通信部(包括接收寄存器)404。

记录设备400具有密码翻译处理部401的控制部403中的命令号管理部2201(2901？)。命令号管理部2901具有命令寄存器2902，以便存储与输出自记录和再现设备300的命令号相对应的命令串。在命令串中，命令号0至y按顺序与执行命令相关联，如图29的右侧所示。命令号管理部2901监视输出自记录和再现设备300的命令号，以便从命令寄存器2902取出相应的命令以便执行。

在存储于命令寄存器2902的命令序列中，用于鉴别处理序列的命令串与前面的命令号0至k相关联，如图29的右侧所示。此外，用于鉴别处理序列的命令串之后的命令号p至s与解密、密钥交换及加密处理命令序列1相关联，以后的命令号u至y与解密、密钥交换及加密处理命令序列2相关联，

如以上就图20中的鉴别过程所述，当将记录设备400安装到记录和再现设备300内时，记录和再现设备300的控制部301将安装命令通过记录设备控制器303传给记录设备400。在接收到命令时，记录设备400使记录设备密码翻译处理部401的控制部403通过通信部404接收命令并清除鉴别标志2903。也就是说，设置未鉴别状态。另外，在从记录和再现设备300向记录设备400供电的情况下，可在电源开时设置未鉴别状态(？)。

然后，记录和再现设备300的控制部301将安装命令传给记录和再现设备密码翻译处理部302。这时，控制部301还会发送记录设备插入端口号。当发送记录设备插入端口号时，即使有多个记录设备400与记录和再现设备300相连，记录和再现设备300也会同时执行与记录设备400的鉴别并将数据传给记录设备且接收来个记录设备的数据。

在接收到安装命令时，记录和再现设备300的记录和再现设备密码翻译处理部302会使使其控制部306清除与记录设备插入端口号相对应的签别标志2904。也就是说，设置成未鉴别的状态。

一旦完成了安装过程，记录和再现设备300的控制部301通过记录设备控制303按始于命令号0的升序顺序地输出命令号。记录设备400命令号管理部2901监视输入自记录和再现设备300的命令号，以

确保它们是始于命令号 0 的顺序输入，并且从命令寄存器 2902 中获得相应的命令，以便执行诸如鉴别处理过程之类的多种处理过程。如果输入的命令号不处于指定的顺序内，则会出错，并且，将命令号接收值重置成初始值，也就是说，将可执行的命令号重置成 0。

在存储在命令寄存器 2092 中的如图 29 所示的命令序列中，告知命令号以便先执行鉴别过程，在这一过程序列之后，存储有解密、密钥交换和加密过程序列。

以下参照图 30 和 31 说明解密、密钥交换和加密过程序列的具体实例。

图 30 示出了如前图 22 所述在将内容从记录和再现设备 300 下载至记录设备 400 时执行的过程的一部分。具体地说，在图 22 中的步骤 59 和 60 之间执行这一过程。

在图 30 中，在步骤 S3001 中，记录设备从记录和再现设备中接收用会话密钥 Kses 加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)。此后，开始图 21 所示的命令串 p 至 s。在鉴别处理命令 0 至 k 业已完成以便将图 29 所示的鉴别标志 2903 和 2904 设置成表示完成之后，开始命令串 p 至 s。命令号管理部 2901 通过仅按始于 0 的升序来接收命令号而确保做到这一点的。

在步骤 S3002 中，记录设备将接收自记录和再现设备的并用会话密钥 Kses 加以加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon) 存储在寄存器内。

在步骤 S3003 中，执行这样过程，它从寄存器中取出用会话密钥 Kses 加以加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)并用会话密钥 Kses 对它们进行解密。

在步骤 S3004 中，执行这样过程，它用存储密钥 Kstr 对用会话密钥 Kses 加以解密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)进行加密。

上述步骤 3002 至 3004 与包括如先前在图 29 所示的命令寄存器中的命令号 p 至 s 内的过程相对应。记录设备密码翻译处理部 401 根据记录设备 400 的命令号管理部 2901 从记录和再现设备 300 中所接收的命令号 p 至 s 顺序执行这些过程。

在步骤 S3005 中，将用存储密钥 Kstr 加以加密的数据(例如块信

息表密钥 Kbit、内容密钥 Kcon)存储进记录设备的存储器内。在这一步骤中，记录和再现设备 300 可从记录设备密码翻译处理部 401 中读出用存储密钥 Kstr 加密的数据，然后将它们存储到记录设备 400 的外部存储器 402 内。

上述步骤 S3002 至 S3004 构成了不间断连续执行的执行序列，例如，即使记录和再现设备 300 在步骤 S3003 的解密过程结束时发出数据读取命令，由于这种读取命令不同于按升序设置在命令寄存器 2902 内的命令号 p 至 s，故命令号管理部 2091 不会接受执行读取。因此，外部设备例如记录和再现设备 300 不能读出源于记录设备 400 中密钥交换的解密数据，从而能防止密钥数据或内容被非法读取。

图 31 示出了图 28 所示的内容再现过程，其中，从记录设备 400 中读出内容并由记录和再现设备 300 对内容进行再现。具体地说，在图 28 的步骤 S73 中执行这一过程。

在图 31 中，在步骤 S101 内，从记录设备 400 的存储器 402 中读出用存储密钥 Kstr 加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)。

在步骤 S3102 中，将从记录设备的存储器中读出的并用存储密钥 Kstr 加以加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon) 存储在寄存器内。在这一步骤中，记录和再现设备 300 可从记录设备 400 的外部存储器 407 中读出用存储密钥 Kstr 加密的数据并将它们存储到记录设备 400 的寄存器内。

在步骤 S3103 中，从寄存器中取出用存储密钥 Kstr 加以加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)并用存储密钥 Kstr 加以解密。

在步骤 S3104 中，用会话密钥 Kses 对用存储密钥 Kstr 加以解密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)进行加密。

上述处理过程步骤 3102 至 3104 与包括在图 29 所述命令寄存器内命令号 u 至 y 中的过程相对应。记录设备密码翻译处理部 406 按记录设备的命令号管理部 2901 从记录和再现设备 300 中接收的命令号 u 至 y 顺序地执行这些过程。

在下一步骤 S3105 中，将用会话密钥 Kses 加以加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)从记录设备传至记录和再现设备。

上述处理过程步骤 3102 至 3104 构成了不间断连续执行的执行序列，例如，即使记录和再现设备 300 在步骤 S3103 的解密过程结束时发出数据读取命令，由于这种读取命令不同于按升序设置在命令寄存器 2902 内的命令号 u 至 y，故命令号管理部 2091 不会接受执行读取。因此，外部设备例如记录和再现设备 300 不能读出源于记录设备 400 中密钥交换的解密数据，从而能防止密钥数据或内容被非法读取。

就图 30 和 31 所示的过程而言，示出了这样的实例，其中，块信息表密钥 Kbit 和内容密钥 Kcon 通过密钥交换来解密和加密，但存储在图 29 所命令寄存器 2902 中的这些命令序列可包括涉及用于内容本身的密钥交换的解密和加密过程。通过密钥交换要加以解密或加密的对象并不限于上述实例。

业已说明了本发明数据处理设备中相互鉴别之后的密钥交换过程。因此，仅在记录和再现设备与记录设备之则的鉴别过程完成之后执行本发明数据处理设备中的密钥交换过程。再有，可防止在密钥交换过程中从外部访问解密的数据，从而能确保内容和密钥数据有提高了的保密性。

(10) 多种内容数据格式以及与各格式相对应的下载和再现过程

在上述实施例中，例如，用于图 3 所示介质 500 或通信装置 600 的数据格式是图 4 所示的格式。用于介质 500 或通信装置 600 的数据格式并不局限于图 4 所的格式，而是最好随内容而定，也就是说，随内容是音乐、图像数据、诸如游戏之类的程序或类似数据而定。以下说明多种数据格式和用于从和自记录设备 400 下载和再现数据的过程。

图 32 至 35 示出了四种不同的数据格式。各图的左侧示出了图 3 所示的介质 500 或通信介质 600 上使用的数据格式，而各图的右侧侧示出了存储在记录设备 400 的外部存储器 402 中的数据中所使用的数据格式。首先提供了图 32 至 35 中所示的数据格式的概要，并且，说明各格式的数据的内容和各格式的数据之间的不同。

图 32 示出了格式类型 0，它与上述内容中的实例所示的有同样的类型。格式类型 0 的特征在于，整个数据被划分成 N 个数据块即块 1 至 N，每个块均具有任意的长度，每个块均是任意加密的，因此，可通过将加密的块和非加密的块即无格式文本块混合到一起而构成数据。

用内容密钥 Kcon 对数据块加密，而内容密钥 Kcon 则是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。块信息密钥 Kbit 也是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。按“(9)相互鉴别之后的密钥交换过程”中所述过程进行这些密钥的交换。

图 33 示出了格式类型 1，其中，如在格式类型 0 中那样，整个数据被划分成 N 个数据块即块 1 至 N，但在 N 个块均有同样的长度方面不同于格式类型 1。用于用内容密钥 Kcon 对块进行加密的过程方面类似于格式类型 0。此外，如在上述格式 0 中那样，内容密钥 Kcon 和块信息密钥 Kbit 是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。与格式 0 不同的是，格式类型 1 具有固定块结构，以简化诸如各块长度之类的结构数据，从而与格式类型 0 相比能减少用于块信息的存储长度。

在图 33 的结构的实例中，各块均包括一组加密的部分和非加密(无格式文本)的部分。如果块的长度和结构是规则的，则在解密过程或类似过程中不需要检查各块长度或结构，从而，能有效地进行解密和加密处理。在格式 1 中，构成各块的部分即加密的部分和非加密(无格式文本)的部分均可被限定为要加以检查的对象，因此，为包含有必须加以检查的部分的块限定内容整体性检查值 ICVi。

图 34 示出了格式类型 2，其特征在于，数据被划分成 N 个数据块即块 1 至 N，所有的块均具有同样的长度，每个块均是用个别块密钥 Kblc 来加密的。各个块密钥 Kblc 均是用内容密钥 Kcon 来加密的，而内容密钥 Kcon 则是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。块信息密钥 Kbit 也是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。

图 35 示出了格式类型 3，其特征在于，数据被划分成 N 个数据块即块 1 至 N，所有的块均具有同样的长度，如在格式类型 2 中那样，每个块均是用个别块密钥 Kblc 来加密的，并且，各个块密钥 Kblc 均是

用内容密钥 Kcon 来加密的，而内容密钥 Kcon 则是用介质上的发布密钥 KdiS 来加密的或在不用内容密钥的情况下用记录设备上的存储密钥 Kstr 来加密的。块信息密钥 Kbit 是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。

以下说明上述格式类型 0 至 3 中的数据的内容。如前所述，数据被大致分成两部分即头标部和内容部。头标部包含内容 ID、使用策略、整体性检查值 A 和 B、总体整体性检查值、块信息表密钥、内容密钥以及块信息表。

使用策略存储有内容的数据长度、其头标长度、其格式类型(下述的格式 0 至 3)、表示内容是包括还是数据的内容类型、确定如在用于从记录设备中下载内容和将内容再现至记录设备的过程的部分中所述那样内容是否仅由特定记录和再现设备使用还是本地化标志、用于内容拷贝或移动处理的许可标志以及用于内容的诸如内容加密算法和模式之类的多种本地化和处理过程信息。

整体性检查值 A: ICVa 用于检查内容 ID 和使用策略并且是用例如图 23 所述的方法生成的。

块信息表密钥 Kbit 用于对块信息表进行加密并且是用是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的，如前所述。

内容密钥 Kcon 用于对内容块进行加密。就格式类型 0 和 1 而言，与块信息表密钥 Kbit 相类似，内容密钥 Kcon 是用介质上的发布密钥 KdiS 来加密的或在被存储到记录设备上时用存储在记录设备的内部存储器中的存储密钥 Kstr 来加密的。就格式类型 2 而言，内容密钥 Kcon 也用于对为各内容块配置的块密钥 Kblc 进行加密。此外，就格式类型 3 而言，不存在内容密钥 Kcon。

块信息表说明与各个块有关的信息并存储有各块的长度和表示是否对块进行了加密的标志即表示是否要对块进行检查(IVC)的信息。如果要对块进行检查，则限定块整体性检查值 ICVi(用于块 i 的整体性检查值)并将其存储在表内。用块信息表密钥 Kbit 对块信息表进行加密。

如果对块进行了加密，则通过每 8 字节对整个无格式文本(解密的文本)作异或操作然后用存储在记录和再现设备 300 的内部存储器 307

中的内容整体性检查值生成密钥 Kicvc 对所获得的值进行加密而生成块整体性检查值即内容整体性检查值 ICVi。此外，如果未对块进行加密，则通过将整个块数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 36 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)生成块整体性检查值。图 36 示出了用于生成内容整体性检查值 ICVi 的结构的一个实例。每个消息 M 均构成了各个由 8 字节解密文本数据或无格式文本数据构成的集合。

就格式类型 1 而言，如果块中的至少一部分是要用整体性检查值 ICVi 来处理的数据即是要加以检查的部分，则为该块限定内容整体性检查值 ICVi。通过每 8 字节对整个无格式文本(解密的文本)作异或操作然后用内容整体性检查值生成密钥 Kicvc 对所获得的数据进行加密而生成用于块 i 的部分 j 的整体性检查值 P-ICVij。此外，如果未对部分 j 进行加密，则通过将整个块数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 36 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)生成块整体性检查值 P-ICVij。

再有，如果块 i 包含有表示要加以检查的具有[ICV 标志=ICV 主题]的一部分，就将用上述方法生成的整体性检查值 P-ICVij 直接用作块整体性检查值 ICVi。如果块 i 包含多个表示要加以检查的具有[ICV 标志=ICV 主题]的部分，则通过按部分号将多个部整体性检查值 P-ICVij 连到一起以获得数据并将整个块数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 37 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)而生成块整体性检查值 P-ICVij。图 37 示出了用于生成内容整体性检查值 ICVi 的结构的一个实例。

不为格式类型 2 或 3 限定块整体性检查值 ICVi。

整体性检查值 B: ICVb 用于检查块信息表密钥、内容密钥和整个块信息表并且是用例如图 24 所述的方法生成的。

总体整体性检查值 ICVt 用于检查全部的前述整体性检查值 A: ICVa 和 B: ICVb 以及包含在要加以检查的各内容块中的整体性检查值 ICVi 并且是通过将系统签名密钥 Ksys 应用于根据诸如整体性检查值 A: ICVa 之类各整体性检查值生成的中间整体性检查值以执行如前图 25

所述的加密过程而生成的。

就格式类型 2 和 3 而言，总体整体性检查值 ICVt 是通过将系统签名密钥 Ksys 应用于中间整体性检查值以执行如前图 25 所述的加密过程而生成的，所述中间整体性检查值则是通过将前述整体性检查值 A: ICVa 和 B: ICVb 连接于内容数据即块 1 中块密钥与最终块之间的整个数据而生成的。图 38 示出了用于生成格式 2 和 3 的总体整体性检查值 ICVi 的结构的一个实例。

如果前述本地化标志置成 1，即表示内容仅能由特定的记录和再现设备所使用，那么，就用总体整体性检查值 ICVt 来代替独有的整体性检查值 ICVdev。就格式类型 0 和 1 而言，生成独有的整体性检查值以检查前述整体性检查值 A: ICVa 和 B: ICVb 以及包含在要加以检查的各内容块中的整体性检查值 ICVi。具体地说，通过将记录和再现设备签名密钥 Kdev 应用于根据诸如整体性检查值 A: ICVa 之类整体性检查值生成的中间整体性检查值而生成独有的整体性检查值 ICVdev，如先前图 25 或 38 所述。

以下参照图 39 至 44 中的流程说明用于将各格式类型 0 至 3 的内容从记录和再现设备下载至记录设备 400 的过程以及记录和再现设备 300 所执行的用于再现来自记录设备 400 的各格式类型 0 至 3 的内容的过程。

首先参照图 39 说明用于下载格式类型 0 或 1 的内容的过程。

例如通过将记录设备 400 安装进图 3 所示的记录和再现设备 300 而开始图 39 所示的过程。在步骤 S101 中，在记录和再现设备与记录设备之间进行相互鉴别，按先前图 20 所述的鉴别流程来执行这一步骤。

如果步骤 S101 中的鉴别过程业已完成以设置鉴别标志，则在步骤 S102 中，记录和再现设备 300 通过读取部 304 从存储有内容数据的介质 500 中读出预定格式的数据，或者，用通信部 305 按预定格式从通信装置 600 中接收数据。然后，记录和再现设备 300 的控制部 301 将数据的头标部发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。

此后，在 S103 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整

体性检查值 A。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥并将内容 ID 和使用策略用作消息的情况下按图 7 所述的 ICV 计算方法来计算整体性检查值 A，如图 23 所示。然后，在步骤 S104 中，存储在头标中的整体性检查值 A 和检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S105。

如前所述，检查值 A、ICVa 用于验证内容 ID 和使用策略尚未被篡改。如果在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥并将内容 ID 和使用策略用作消息的情况下按图 7 所述 ICV 计算方法计算出的整体性检查值 A 等于存储在头标中的检查值 ICVa，则可判断出内容 ID 和使用策略未被篡改。

在步骤 S105 中，记录和再现设备加密处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 获得或生成发布密钥 Kdis。如在图 22 的步骤 S53 中那样，用例如用于发布密钥的主密钥 MKdis 生成发布密钥 Kdis。

在步骤 S106 中，记录和再现设备密码翻译处理部 302 的控制部 306 用记录和再现设备密码翻译处理部 302 的加密/解密部 308 及所生成的发布密钥 Kdis 对存储在数据的头标部中的块信息表密钥 Kbit 和内容密钥 Knon 进行解密，所述数据是通过读取部 304 从介质 500 中获得的或者是通过通信部 305 从通信装置 600 中接收的。

在步骤 S107 中，记录和再现设备密码翻译处理部 302 的控制部 306 用记录和再现设备密码翻译处理部 302 的加密/解密部 308 借助解密的块信息表密钥 Kbit 对块信息表密钥进行解密。

再有，在步骤 108 中，记录和再现设备密码翻译处理部 302 的控制部 306 根据块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT) 计算整体性检查值 B(ICVb')。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥而生成整体性检查值 B，以便根据 DES 对经异或运算的值进行解密，图 24 所示。经异或运算的值包括块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)。在步骤 S109 中，整体性检查值 B 和头标中的检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S110。

如前所述，检查值 B、ICVb 用于块信息表密钥 Kbit、内容密钥 Kcon 和块信息表尚未被篡改。如果通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥、将块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)分成 8 字节的段、对这些数据作异或运算、并根据 DES 对作了异或运算的数据进行加密从而生成的整体性检查值 B 等于存储在头标中的检查值 ICVb，则可判断出块信息表密钥 Kbit、内容密钥 Kcon 和块信息表未被篡改。

在步骤 S110 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算中间整体性检查值。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的总体整体性检查值生成密钥 Kicvt 用作密钥并将整体性检查值 A 和 B 以及所有保存的内容整体性检查值用作消息的情况下按图 7 所述的 ICV 计算方法来计算上述中间值。所生成的中间整体性检查值按需存储在记录和再现设备 300 的记录和再现设备密码翻译处理部 302 内。

在步骤 S111 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算总体整体性检查值 ICVt'。如图 25 所示，通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的系统签名密钥 Ksys 用作密钥而生成总体整体性检查值 ICVt，以便根据 DES 对中间整体性检查值进行解密。然后，在步骤 S112 中，所生成的总体整体性检查值 ICVt 和在步骤 S112 中存储在头标中的 ICVt'一起作比较，如果它们相等，则处理过程前进至步骤 S113。

如前在图 4 中所述，总体整体性检查值 ICVt 用于验证所有整体性检查值 ICVa 和 ICVb，以及用于各内容块的整体性检查值未被篡改。因此，如果通过上述过程生成的总体整体性检查值等于存储在头标中的整体性检查值 ICVt，则可判断出所有整体性检查值 ICVa 和 ICVb 以及用于各内容块的整体性检查值未被篡改。

然后，在步骤 S113 中，记录和再现设备 300 的控制部 301 从块信息表(BIT)中取出内容块信息并检查是否要验证任何的内容块。如果要验证任一内容块，则内容整体性检查值已被存储在头标的块信息内。

如果要验证任一内容块，则在步骤 114 中，控制部 301 通过用记录和再现设备 300 的读取部 304 从介质 500 中读出内容块或者通过记录和再现设备 300 的通信部 305 读出接收自通信装置 600 的内容块，并将内容块发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。在接收到内容块时，记录和再现设备 300 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算内容整体性检查值 ICVi'。

如果对块进行了加密，则通过用内容密钥 Kcon 在 DES CBC 模式下对输入内容块加以解密、按每 8 字节对解密的文本作异或操作，然后用存储在记录和再现设备 300 的内部存储器 307 中的内容整体性检查值生成密钥 Kicvc 对所生成的内容中间值进行加密从而生成块整体性检查值 ICVi。此外，如果未对块进行加密，则通过将整个块数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 36 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)生成块整体性检查值。

在步骤 S115 中，记录和再现设备 300 的控制部 306 将这一内容整体性检查值与在步骤 S102 中接收自记录和再现设备 300 的控制部 301 的内容块中的 ICV 作比较，并将结果传给记录和再现设备 300 的控制部 301。在接收到上述结果且在已成功验证的情况下，记录和再现设备 300 的控制部 301 取出下一个要加以验证的内容块并使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 验证该内容块。重复相类似的验证过程，直至验证了所有的内容块(步骤 S116)。

在这方面，如果检查值在步骤 104、109、112 和 115 中任何一个步骤中不相等，则会出错，从而结束下载过程。

然后，在步骤 S117 中，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 通过使用在相互鉴别过程中可共享的会话密钥 Kses 对在步骤 S106 中解密的块信息表密钥 Kbit 和内容密钥 Kcon 进行加密。记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读取块信息表密钥 Kbit 和内容密钥 Kcon，然后将它们通过记录和再现设备 300 的记录设备控制器 303 传给记录设备 400。

在步骤 S118 中，在接收到传送自记录和再现设备 300 的块信息表密钥 Kbit 和内容密钥 Kcon 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用在相互鉴别过程中可共享的会话密钥 Kses 对接收到的数据进行解密并用存储在记录设备密码翻译处理部 401 的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对解密的数据重新加密。然后，记录和再现设备 300 的控制部 301 通过记录和再现设备 300 的记录设备控制器 303 从记录设备 400 中读出块信息表密钥 Kbit 和内容密钥 Kcon，块信息表密钥 Kbit 和内容密钥 Kcon 是用存储密钥 Kstr 来重新加密的。也就是说，用用发布密钥 Kdis 加以加密的块信息表密钥 Kbit 可与内容密钥 Kcon 相交换。

在步骤 S119 中，记录和再现设备 300 的控制部 301 从数据的头标部内的使用策略中取出本地化字段，以便判断下载的内容是否是仅用于这一记录和再现设备 300。如果本地化字段置成 1，则下载的内容仅用于这一记录和再现设备 300。如果本地化字段置成 0，则下载的内容也可由其它类似记录和再现设备 300 所使用。如果判断的结果显示出本地化字段置成 1，则处理过程前进至步骤 S120。

在步骤 S120 中，记录和再现设备 300 的控制部 301 使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 计算记录和再现设备所独有的整体性检查值。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的记录和再现设备签名密钥 Kdev 用作密钥而生成记录和再现设备所独有的整体性检查值，以便根据 DES 对中间整体性检查值进行解密，在步骤 S110 中生成上述中间整体性检查值。计算出的为记录和再现设备所独有的整体性检查值 ICVdev 可代替总体整体性检查值 ICVt。

如上所述，系统签名密钥 Ksys 用于将共用签名或 ICV 附加给发布系统，并且，记录和再现设备签名密钥 Kdev 随记录和再现设备而变并且可由记录和再现设备所使用，以便附加签名或 ICV。也就是说，用系统签名密钥 Ksys 签署的数据可由具有同样系统签名密钥的系统(记录和再现设备)来成功地检查，也就是说，这种数据具有同样的总体整体性检查值，从而能得以共享。但是，如果用记录和再现设备签名密钥 kdev 来签署数据，由于这种签名密钥为记录和再现设备所独有，所以，即便将记录设备插进另一个记录和再现设备中之后试图再现用记录和

再现设备签名密钥 Kdev 签署的数据（即在签署之后存储在记录设备中的数据），也不能再现这些数据，也就是说，会因不相等的为记录和再现设备所独有的整体性检查值 ICVdev 而出现错误。在本发明的数据处理设备中，设置本地化字段能将内容任意地设置在整个系统内共享或仅由特定的记录和再现设备所使用。

然后，在步骤 S121 中，记录和再现设备 300 的控制部 301 使记录和再现设备密码翻译处理部 302 形成存储数据格式。如前所述，在头标的使用策略(见图 5)中设置三种格式类型 0 至 3 中的一种，因此，根据所设置的类型依照前述图 32 至 35 之一的右侧中的存储格式来形成数据。图 39 所示的流程用于格式 0 或 1，因此，将数据形成为图 32 和 33 中的格式之一。

一旦在步骤 S121 中完成了存储数据格式，记录和再现设备 300 的控制部 301 在步骤 S122 中将内容存储到记录设备 400 的外部存储器 402 内。

业已说明了如何执行用于下载格式 0 或 1 的内容数据的过程。

以下参照图 40 说明用于下载格式 2 的内容数据的过程。将侧重于与上述用于下载格式 0 或 1 的内容数据的过程的不同之处。

步骤 S101 至 S109 与上述用于下载格式 0 或 1 的内容数据的过程相类似，从而略去对它们的说明。

由于格式类型 2 没有如前所述那样限定的内容整体性检查值 ICVi，故块信息表不包含整体性检查值 ICVi。格式类型 2 中的中间整体性检查值是通过将系统签名密钥 Ksys 应用于中间整体性检查值以执行加密过程而生成的，所述中间整体性检查值则是通过将前述整体性检查值 A 和 B 连接于第一块的前部数据(块 1 中的块密钥)与最终块之间的整个数据而生成的。

因此，在用于下载格式 2 的数据的过程中，在步骤 S151 中读出内容数据，并在步骤 S152 中根据整体性检查值 A 和 B 以及读出的内容数据生成中间整体性检查值。这方面，即使内容数据已加密，也不对它们解密。

就格式类型 2 而言，与前述用于格式类型 0 或 1 的过程相反，省略了用于对块数据解密和比较内容整体性检查值的过程，以便提高处理速度。

步骤 S111 和后续步骤的过程与用于格式类型 0 或 1 的过程相类似，因此略去了对它们的说明。

业已说明了如何执行用于下载格式类型 2 的内容数据的过程。如前所述，与前述用于格式类型 0 或 1 的过程相反，用于下载格式类型 2 的内容数据的过程省略了用于对块数据解密和比较内容整体性检查值的过程，以便提高处理速度，因此，这种格式适于对音乐数据或必须实时执行的类似数据的处理。

以下参照图 41 说明用于下载格式 3 的内容数据的过程。以下说明将侧重于与上述用于格式 0、1 和 2 下载过程的不同之处。

步骤 S101 至 S105 与上述用于格式 0、1 和 2 下载过程的相类似。

用于格式类型 3 的过程基本上具有与用于格式类型 2 的过程相共同的多种特征，但是，不同之处在于，格式类型 3 没有内容密钥，因为，块密钥 Kblc 在用存储密钥 Kstr 加密之后存储在记录设备内。

以下说明侧重于用于格式类型 3 的下载过程与用于格式类型 2 的下载过程之间的不同。在格式类型 3 的情况下，在步骤 S161 中，于步骤 S105 之后，对块信息表密钥解密。记录和再现设备密码翻译处理部 302 的控制部 306 用记录和再现设备密码翻译处理部 302 的加密/解密部 308 及在步骤 105 中所生成的发布密钥 Kdis 对存储在数据的头标部中的块信息表密钥 Kbit 进行解密，所述数据是通过读取部 304 从介质 500 中获得的、或者是通过通信部 305 从通信装置 600 中接收的。在格式类型 3 的情况下，数据不包含内容密钥 Kcon，因此，不执行用于对内容密钥 Kcon 解密的过程。

在下一步骤 S107 中，在步骤 S161 中解密的块信息表密钥 Kbit 用于对块信息表进行解密，并且，在步骤 S162 中，记录和再现设备密码翻译处理部 302 的控制部 306 根据块信息表密钥 Kbit 和块信息表(BIT)生成整体性检查值 B(ICVb')。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥而生成整体性检查值 B，以便根据 DES 对经异或运算的值进行解密，经异或运算的值包括块信息表密钥 Kbit 和块信息表(BIT)。然后，在步骤 S109 中，整体性检查值 B 和头标中的检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S151。

在格式类型 3 的情况下，检查值 B、ICVb 用于验证块信息表密钥

Kbit 和块信息表未被篡改。如果所生成的整体性检查值 B 等于存储在头标中的检查值 ICVb，则可判断出块信息表密钥 Kbit 和块信息表未被篡改。

步骤 S151 至步骤 S112 与用于格式类型 2 的过程步骤相类似，因此省略了对它们的说明。

在步骤 S163 中，用在步骤 S105 中生成的发布密钥 Kdis 对包含在于步骤 S151 中读出的内容数据内的块密钥 Kblc 进行解密。

然后，在步骤 S164 中，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 通过使用在相互鉴别过程中可共享的会话密钥 Kses 对在步骤 S161 中解密的块信息表密钥 Kbit 和在步骤 S163 中解密的块密钥 Kblock 进行加密。记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读取块信息表密钥 Kbit 和块密钥 Kblc，然后将这些数据通过记录和再现设备 300 的记录设备控制器 303 传给记录设备 400。

在步骤 S165 中，在接收到传送自记录和再现设备 300 的块信息表密钥 Kbit 和块密钥 Kblc 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用在相互鉴别过程中可共享的会话密钥 Kses 对接收到的数据进行解密并用存储在记录设备密码翻译处理部 401 的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对解密的数据重新加密。记录和再现设备 300 的控制部 301 通过记录和再现设备 300 的记录设备控制器从记录设备 400 中读出块信息表密钥 Kbit 和块密钥 Kblc，块信息表密钥 Kbit 和块密钥 Kblc 是用存储密钥 Kstr 来重新加密的。也就是说，用发布密钥 Kdis 在开始加以加密的块信息表密钥 Kbit 和块密钥 Kblc 可用用存储密钥 Kstr 重新加密的块信息表密钥 Kbit 和块密钥 Kblc 来代替。

后续步骤 S119 至步骤 S122 与用于格式类型 0、1 和 2 的步骤相类似，因此略去了对它们的说明。

业已说明了用于下载格式类型 3 的内容数据的过程方面。如前所述，用于格式类型 2 的下载过程如用于格式类型 2 的过程那样略去了用于对块数据解密和比较内容整体性检查值的过程，以便加快处理，因此，格式类型 3 适于处理诸如音乐数据之类需要实时处理的数据。

此外，由于块密钥 Kblc 能确定加密内容受保护的范围，故与格式类型 2 相比，能获得有所提高的保密性。

以下参照图 42 至 45 的流程说明用于再现来自记录和再现设备 300 的记录设备 400 的各格式类型 0 至 3 的数据的过程。

首先，参照图 42 说明用于再现格式类型 0 的数据的过程。

步骤 S201 与记录和再现设备和记录设备之间的鉴别过程相对应，并且是按图 20 中所述的鉴别流程来执行的。

一旦步骤 S201 中的鉴别过程业已完成以设置鉴别标志，则在步骤 S202 中，记录和再现设备 300 从记录设备 400 中读出预定格式的数据的头标并将其发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。

此后，在 S203 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算整体性检查值 A。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 A 生成密钥 Kicva 用作密钥并将内容 ID 和使用策略用作消息的情况下计算整体性检查值 A，如图 23 所示。然后，在步骤 S204 中，整体性检查值 A 和存储在头标中的检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S205。

检查值 A、ICVa 用于验证内容 ID 和使用策略未被篡改。如果计算出的整体性检查值 A 等于存储在头标中的检查值 ICVa，则可判断出内容 ID 和使用策略未被篡改。

在步骤 S205 中，记录和再现设备的控制部 306 从读出的头标部中取出块信息表密钥 Kbit 和内容密钥 Knon，并通过记录和再现设备 300 的记录设备控制器 303 将它们发送给记录设备 400，所述块信息表密钥 Kbit 和内容密钥 Knon 是用记录设备所独有的存储密钥 Kstr 来加密的。

在接收到传送自记录和再现设备 300 的块信息表密钥 Kbit 和内容密钥 Knon 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用存储在记录设备密码翻译处理部 401 的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对接收到的数据进行解密并用在相互鉴别过程中可共享的会话密钥 Kses 对解密的数据重新加密。这一过程如先前在(9)相互鉴别之后的密钥交换过程中详细所述。

在步骤 S206 中，记录和再现设备 300 的控制部 301 通过记录和再现设备 300 的记录设备控制器 303 从记录设备 400 中接收块信息表密钥 Kbit 和块密钥 Kblc，块信息表密钥 Kbit 和块密钥 Kblc 是用会话密钥 Kses 来重新加密的。

在步骤 S207 中，记录和再现设备 300 的控制部 301 将接收到的用用会话密钥 Kses 来重新加密的块信息表密钥 Kbit 和内容密钥 Kcon 发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。在接收到用会话密钥 Kses 重新加密的块信息表密钥 Kbit 和内容密钥 Knon 时，记录和再现设备 300 的密码翻译处理部 302 就使记录和再现设备密码翻译处理部 302 的加密/解密部 308 用在相互鉴别过程中可共享的会话密钥 Kses 对密钥 Kbit 和 Kcon 解密。

再有，在步骤 S208 中，解密的块信息表密钥 Kbit 用于对在步骤 S202 中读出的块信息。记录和再现设备 300 的记录和再现设备密码翻译处理部 302 用包含在步骤 S202 读出的头标中的块信息表密钥 Kbit、内容密钥 Kcon 和块信息表 BIT 来代替解密的块信息表密钥 Kbit、内容密钥 Kcon 和块信息表 BIT，以便保存包含在步骤 S202 读出的头标中的块信息表密钥 Kbit、内容密钥 Kcon 和块信息表 BIT。此外，记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读出解密的块信息表 BIT。

此外，在步骤 S209 中，记录和再现设备密码翻译处理部 302 的控制部 306 根据块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT) 生成整体性检查值 B(ICVb')。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥而生成整体性检查值 B，以便根据 DES 对经异或运算的值进行解密，经异或运算的值包括块信息表密钥 Kbit、内容密钥 Kcon 和块信息表(BIT)。然后，在步骤 S210 中，整体性检查值 B 和头标中的检查值 ICVa 一起作比较，如果它们相等，则处理过程前进至步骤 S211。

检查值 B、ICVb 用于块信息表密钥 Kbit、内容密钥 Kcon 和块信息表未被篡改。如果生成的整体性检查值 B 等于存储在头标中的检查值 ICVb，则可判断出存储在记录设备 400 中块信息表密钥 Kbit、内容密钥 Kcon 和块信息表未被篡改。

在步骤 S211 中，记录和再现设备密码翻译处理部 302 的控制部 306

使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算中间整体性检查值。在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的总体整体性检查值生成密钥 Kicvt 用作密钥并将经验证的整体性检查值 A 和 B 以及块信息表中的所有内容整体性检查值用作消息的情况下按图 7 所述的 ICV 计算方法来计算上述中间值，如图 25 所示。在这方面，所生成的中间整体性检查值按需存储在记录和再现设备 300 的记录和再现设备密码翻译处理部 302 内。

在步骤 S212 中，记录和再现设备 300 的控制部 301 从包含在数据（该数据是从记录设备 400 的外部存储器 402 读出的）的头标部内的使用策略中取出本地化字段，以判断要加以再现的内容是仅用于这一记录和再现设备 300(在这种情况下，将本地化字段置成 1)还是也可由其它相类似记录和再现设备 300 所使用(在这种情况下，将本地化字段置成 0)。如果判断的结果显示出本地化字段置成 1，也就是说，再现的内容仅用于这一记录和再现设备 300，则处理过程前进至步骤 S213。如果本地化字段置成 0，也就是说，再现的内容也可由其它相类似记录和再现设备 300 所使用，则处理过程前进至步骤 S215。步骤 S211 的过程由密码翻译处理部 302 来执行。

在步骤 S213 中，记录和再现设备 300 的控制部 301 使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 计算为记录和再现设备所独有的整体性检查值 ICVdev'。如图 25 所示，通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的记录和再现设备签名密钥 Kdev 用作密钥而生成记录和再现设备所独有的整体性检查值 ICVdev'，以便根据 DES 对中间整体性检查值进行解密，所述中间整体性检查值是在步骤 S58 中保存的。

然后，在步骤 S214 中，在步骤 S219 中计算出的为记录和再现设备所独有的整体性检查值 ICVdev'和在步骤 S202 中读出的头标内的 ICVdev 一起作比较，如果它们相等，则处理过程前进至步骤 S217。

另一方面，在步骤 S215 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算总体整体性检查值。通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的系统签名密钥 Ksys 用作密钥而生成总体整体性检查值，以便根据 DES 对中间整体性检查值进行解密，如图 25

所示。在步骤 S216 中，所生成的总体整体性检查值 ICVt'和头标内的 ICVt 一起作比较，如果它们相等，则处理过程前进至步骤 S217。

总体整体性检查值 ICVt 和记录和再现设备所独有的整体性检查值 ICVdev 用于验证所有整体性检查值 ICVa 和 ICVb 以及用于各内容块的整体性检查值未被篡改。因此，如果通过上述过程生成的总体整体性检查值等于存储在头标中的整体性检查值 ICVt，则可判断出所有用于各内容块的整体性检查值未被篡改。

然后，在步骤 S217 中，记录和再现设备 300 的控制部 301 从记录设备 400 中读出块数据。再有，在步骤 S218 中，判断数据是否已加密，如果数据已加密，记录和再现设备 300 的密码翻译处理部 302 就对块数据解密。如果数据尚未加密，则处理过程跳过步骤 S219 并前进至 S220。

在步骤 220 中，记录和再现设备 300 的控制部 301 根据块信息表(BIT)中的内容块信息表检查是否要验证任何的内容块。如果要验证任一内容块，则内容整体性检查值已被存储在头标的块信息内。在这种情况下，在步骤 S221 计算出用于该内容块的内容整体性检查值 ICVi。如果不要验证内容块，则处理过程跳过步骤 S221 和 S222 并前进至 S223。

如果如图 36 所示对块进行了加密，则通过用内容密钥 Kcon 在 DES CBC 模式下对输入内容块加以解密、按每 8 字节对解密的文本作异或操作以生成内容中间值然后用存储在记录和再现设备 300 的内部存储器 307 中的内容整体性检查值生成密钥 Kicvc 对所获得值进行加密而生成块整体性检查值 ICVi'。 此外，如果未对块进行加密，则通过将整个数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 36 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)生成块内容整体性检查值。

在步骤 S222 中，记录和再现设备密码翻译处理部 302 的控制部 306 将所生成的内容整体性检查值 ICVi'与在步骤 S202 中接收自记录和再现设备 300 的内容块中的 ICVi 作比较，并将结果传给记录和再现设备 300 的控制部 301。在接收到上述结果且在已成功验证的情况下，在步骤 S223 中记录和再现设备系统的 RAM 中用于执行(再现)的内容无格式数据。记录和再现设备 300 的控制部 301 取出下一个要加以验证的内

容块并使记录和再现设备 300 的记录和再现设备密码翻译处理部 302 验证该内容块。重复相类似的验证过程和 RAM 存储过程，直至验证了所有的内容块(步骤 S224)。

如果检查值在步骤 S204、S210、S214、S216 和 S222 中任何一个步骤中不匹配，则会出错，从而结束再现过程。

当在步骤 S224 中判断出读出了所有的块，则处理过程前进至步骤 S225 以开始执行和再现内容(程序或数据)。

业已说明了用于再现格式类型 0 的内容数据的过程方面。

以下参照图 43 说明下载格式类型 1 的内容数据的过程。以下说明侧重于与上述用于格式类型 0 的下载过程的不同之处。

从步骤 S201 至 S217 的过程与上述用于格式 0 的下载过程相类似，从而略去对它们的说明。

就格式类型 1 而言，在步骤 S231 中，对加密的部分解密，以生成部分 ICV。在步骤 S232 中，生成 ICVi'。如前所述，在格式类型 1 的情况下，如果块中的至少一部分包含要用整体性检查值 ICVi 来验证的数据，则为该块限定内容整体性检查值 ICVi。如果已对部分 j 进行加密，则通过每 8 字节对整个无格式文本(解密的文本)作异或操作并用内容整体性检查值生成密钥 Kicvc 对所获得的值进行解密而生成用于块 i 的部分 j 的整体性检查值 P-ICVij。此外，如果未对部分 j 进行加密，则通过将整个数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 36 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)而生成块整体性检查值 P-ICVij。

再有，如果块 i 仅包含有表示要加以检查的具有[ICV 标志=ICV 主题]的一部分，就将用上述方法生成的整体性检查值 P-ICVij 直接用作块整体性检查值 ICVi。如果块 i 包含多个表示要加以检查的具有[ICV 标志=ICV 主题]的部分，则通过按部分号将多个部整体性检查值 P-ICVij 连到一起以获得数据并将整个块数据(无格式文本)按每次输入 8 字节的方式顺序地输入给图 36 所示的篡改检查值生成函数(用内容整体性检查值生成密钥 Kicvc 的 DES-CBC-MAC)而生成块整体性检查值 P-ICVij。这与图 37 所说明的相同。

就格式类型 1 而言，在步骤 S222 通过上述过程生成的内容整体性检查值经历比较。下一步骤 S223 和后续步骤中的过程与用于格式类型

0 的相类似，故略去了对它们的说明。

以下参照图 44 说明用于再现格式类型 2 的内容数据的过程。以下说明侧重于与上述用于格式类型 0 和 2 的再现过程的不同之处。

步骤 S201 至 S210 与述用于格式类型 0 和 2 的再现过程中的相类似，故略去了对它们的说明。

就格式类型 2 而言，不执行就格式类型 0 和 1 所执行的步骤 S211 至 S216 的过程。此外，格式类型 2 不具有内容整体性检查值，故不执行就格式类型 0 和 1 所执行的内容整体性检查值验证。

在用于格式类型 2 的数据再现过程中，在用于验证整体性检查值 B 的步骤 S210 之后，处理过程前进至步骤 S217，其中，在记录和再现设备 300 的控制部 301 的控制下读出块数据。在步骤 S241 中，记录和再现设备 300 的密码翻译处理部 306 对包含在块数据中的块密钥 Kblc 进行解密。存储存记录设备 400 中的块密钥 Kblc 用如图 34 所示的内容密钥 Kcon 来加密并因此而用在前一步骤 S207 中解密的内容密钥 Kcon 来解密。

在步骤 S242 中，在步骤 S241 中解密的块密钥 Kblc 用于对块数据进行解密。在步骤 S243 中，执行并再现内容(程序或数据)。对所有的块都重复从步骤 S217 至 S243 的过程。当在步骤 S244 中判断出读出了所有的块，就结束再现过程。

如前所述，用于格式类型 2 的过程略去了验证诸如总体整体性检查值之类的整体性检查值的过程。因此能提供适于高速执行解密处理的结构以及适于处理诸如需要实时处理的音乐数据之类的格式。

以下参照图 45 说明用于再现格式类型 3 的内容数据的过程。以下说明侧重于与上述用于格式类型 0、1 和 2 的再现过程的不同之处。

用于格式类型 3 的过程基本上具有与用于格式类型 2 的过程相共同的多种特征，但是，不同之处在于，如图 35 所述，格式类型 3 没有内容密钥，因为，块密钥 Kblc 在用存储密钥 Kstr 加密之后存储在记录设备内。

在步骤 S201 与 S210 之间，步骤 S251、S252、S253 和 S254 中的过程与用于格式 0、1 和 2 的相应过程相反配置成略去使用内容密钥。

在步骤 S251 中，记录和再现设备 300 的控制部 301 从读出的头标中取出用记录设备所独有的存储密钥 Kstr 所加密的块信息表密钥

Kbit，然后通过记录和再现设备 300 的记录设备控制器 303 将该密钥发送给记录设备 400。

在接收到传送自记录和再现设备 300 的块信息表密钥 Kbit 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用存储在记录设备密码翻译处理部 401 的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对接收到的数据进行解密，然后用在相互鉴别过程中可共享的会话密钥 Kses 对解密的数据重新加密。这一过程如先前在(9)相互鉴别之后的密钥交换过程中详细所述。

在步骤 S252 中，记录和再现设备 300 的控制部 301 通过记录和再现设备 300 的记录设备控制器 303 从记录设备 400 中接收块信息表密钥 Kbit，块信息表密钥 Kbit 是用会话密钥 Kses 来重新加密的。

在步骤 S253 中，记录和再现设备 300 的控制部 301 将接收到的用会话密钥 Kses 来重新加密的块信息表密钥 Kbit 发送给记录和再现设备 300 的记录和再现设备密码翻译处理部 302。在接收到用会话密钥 Kses 重新加密的块信息表密钥 Kbit 时，记录和再现设备 300 的密码翻译处理部 302 就使记录和再现设备密码翻译处理部 302 的加密/解密部 308 用在相互鉴别过程中可共享的会话密钥 Kses 对块信息表密钥 Kbit 解密。

再有，在步骤 S208 中，解密的块信息表密钥 Kbit 用于对在步骤 S202 中读出的块信息。记录和再现设备 300 的记录和再现设备密码翻译处理部 302 用包含在步骤 S202 读出的头标中的块信息表密钥 Kbit 和块信息表 BIT 来代替解密的块信息表密钥 Kbit 和块信息表 BIT，以便保存包含在步骤 S202 读出的头标中的块信息表密钥 Kbit 和块信息表 BIT。此外，记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读出解密的块信息表 BIT。

此外，在步骤 S254 中，记录和再现设备密码翻译处理部 302 的控制部 306 根据块信息表密钥 Kbit 和块信息表(BIT) 生成整体性检查值 B(ICVb')。如图 24 所示，通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值 B 生成密钥 Kicvb 用作密钥而生成整体性检查值 B，以便根据 DES 对经异或运算的值进行解密，经异或运算的值包括块信息表密钥 Kbit 和块信息表(BIT)。然后，在步

骤 S210 中，整体性检查值 B 和头标中的检查值 ICVb 一起作比较，如果它们相等，则处理过程前进至步骤 S211。

在格式类型 3 的情况下，在存储到记录设备中时，还用存储密钥对块密钥加密，从而需要记录检查值 400 用存储密钥和会话密钥执行解密过程，而且还需要记录和再现设备 300 用会话密钥执行解密过程。这一系列步骤对应于步骤 S255 和 S256 所示的处理步骤。

在步骤 S255 中，记录和再现设备 300 的控制部 301 从读出的头标中取出用记录设备所独有的存储密钥 Kstr 所加密的已在步骤 S217 中读出的块密钥 Kblc，然后通过记录和再现设备 300 的记录设备控制器 303 将该密钥发送给记录设备 400。

在接收到传送自记录和再现设备 300 的块密钥 Kblc 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用存储在记录设备密码翻译处理部 401 的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对接收到的数据进行解密，然后用在相互鉴别过程中可共享的会话密钥 Kses 对解密的数据重新加密。这一过程如先前在(9)相互鉴别之后的密钥交换过程中详细所述。

在步骤 S256 中，记录和再现设备 300 的控制部 301 通过记录和再现设备 300 的记录设备控制器 303 从记录设备 400 中接收块密钥 Kblc，块密钥 Kblc 是用会话密钥 Kses 来重新加密的。

在步骤 S257 中，记录和再现设备 300 的密码翻译处理部 306 用用会话密钥 Kses 对块密钥 Kblc 进行解密。

在步骤 S242 中，在步骤 S257 中解密的块密钥 Kblc 用于对块数据进行解密。在步骤 S243 中，执行并再现内容(程序或数据)。对所有的块都重复从步骤 S217 至 S243 的过程。当在步骤 S244 中判断出读出了所有的块，就结束再现过程。

业已说明了用于再现格式类型 3 的内容的过程。格式类型 3 类似于格式类型 2，因为，略去了用于验证总体整体性检查值的过程，但是，由于包括了用于交换块密钥的过程，故格式类型 3 提高了有较保密程度的处理结构。

(11)内容提供者所执行的用于生成检查值(ICV)的过程方面

在上述实施例中，在下载和再现内容的过程中执行用多种整体性检查值 ICV 的验证过程。以下说明用于生成整体性检查值 ICV 的过程

方面。

首先，简要说明上述实施例中说明的各个整体性检查值。下述整体性检查值 ICV 用于本发明的数据处理设备。

整体性检查值 A，ICVa：用于验证内容数据中的内容 ID 和使用策略未被篡改的整体性检查值。

整体性检查值 B， ICVb：用于验证块信息表密钥 Kbit、内容密钥 Kcon 以及块信息表未被篡改的整体性检查值。

内容整体性检查值 ICVi：用于验证内容的各内容块尚未被篡改的内容整体性检查值。

总体整体性检查值 ICVt；用于验证整体性检查值 ICVa、整体性检查值 ICVb、用于内容块的所有整体性检查值未被篡改的整体性检查值。

记录和再现设备所独有的整体性检查值 ICVdev：在本地化字段置成 1 即内容仅用于特定记录和再现设备的情况下用总整体性检查值 ICVt 来代替的并且可生成为用于包含在要加以检查的各内容块中的上述整体性检查值 A：ICVa、整体性检查值 B：ICVb 和整体性检查值 ICVi 的整体性检查值的整体性检查值。

依照格式的不同，整体性检查值 ICVt 和 ICVdev 不仅检查用于各内容块的检查值而且检查内容本身。

上述各整体性检查值用于本发明的数据处理检查值。在这些整体性检查值中，整体性检查值 A 和 B、总体整体性检查值以及内容整体性检查值均是由用于提供内容数据的内容提供者或以要加以验证的数据为基础的内容管理者例如如图 32 至 35 和 6 所示那样所产生的并在被提供给记录和再现设备 300 的用户之前连同内容存储在数据内。当将内容下载至记录设备或再现来自记录设备的内容时，记录和再现设备的用户即内容用户根据要验证的各数据生成验证 ICV，以便将它们与存储的 ICV 作比较 ICVdev。此外再现设备所独有的整体性检查值 ICVdev 可用总体整体性检查值 ICVt 来代替并在示出了内容仅可由该记录和再现设备所使用的情况下存储在记录设备内。

在上述实施例中，生成整体性检查值的过程主要是以 DES-CBC 为基础的。但是，本发明并不局限于上述方式，而是包括多种 ICV 生成和验证过程方面。具体地说，就内容提供者或管理者与内容用户的关

系而言，可以有以下的多种 ICV 生成和验证过程结构。

图 46 至 48 是用于说明整体性检查值 ICV 的生成器所执行的生成过程以及验证器执行的验证过程。

图 46 示出了这样的结构，其中，例如，是内容提供者或管理者的 ICV 生成器根据上述实施例中所述的 DES-CBC 执行用于生成 ICV 的过程，然后将生成的 ICV 连同内容提供给记录和再现设备的用户即验证器。在这种情况下，就验证过程而言，记录和再现设备的用户即验证者需要例如存储在图 18 所示的内部存储器 307 中的密钥，以便生成相应的整体性检查值。是内容用户的验证器(记录和再现设备的用户)用存储在内部存储器 307 中的整体性检查值生成密钥将 DES-CBC 应用于要加以验证的数据，以便生成整体性检查值，然后将这些值与存储的整体性检查值作比较。在这种情况下，每个整体性检查值生成密钥都配置成能以保密的方式由 ICV 创建者与验证器所共享。

图 47 示出了这样的结构，其中，是内容提供者或管理者的 ICV 创建者用公共密钥密码系统的数字签名生成 ICV，然后将生成的 ICV 连同内容提供给内容用户即验证器，并且，内容用户即验证器存储有 ICV 创建者的公共密钥并用该密钥验证 ICV。在这种情况下，ICV 创建者的由内容用户(记录和再现设备用户)所持有的公共密钥，即验证器不需保密，从而更易于管理。因此，这方面适用于在高保密管理层次上进行 ICV 生成和管理，例如适用于在一个实体中执行的 ICV 生成和管理中。

在图 48 中，是内容提供者或管理者的 ICV 创建者用公共密钥密码系统的数字签名生成 ICV，然后将生成的 ICV 连同内容提供给内容用户即验证器，并且，还将由用于验证的验证器所使用的公共密钥存储在公共密钥证书(例如见图 14)，然后将该密钥提供给记录和再现设备用户即验证器。就多个 ICV 创建者而言，每个创建者均具有密钥管理中心创建数据(公共密钥证书)，以便保证公共密钥的有效性。

是 ICV 验证器的内容用户具有密钥管理中心的公共密钥。验证器用密钥管理中心的公共密钥验证公共密钥证书，如果确认了有效性，则取出存储在公共密钥证书中 ICV 创建者的公共密钥。验证器还用取出的 ICV 创建者的公共密钥验证 ICV。

如果存在有多个 ICV 创建者，并且，如果用于管理这些创建者的中心具有已建立起来的管理系统，则这种方法是一种有用的方面。

(12)用于根据主密钥生成密码翻译处理过程密钥的结构

以下说明用于根据主密钥生成多种密码翻译处理过程密钥的结构，该结构是本发明数据处理系统的特征。

如前参照图 18 所示，本发明数据处理设备的记录和再现设备 300 的内部存储器存储有多个主密钥，每个主密钥都例如用于生成鉴别密钥 Kake(见等式 3)或发布密钥 Kdis(见等式 4)。

当在两个实体即内容提供者与内容提供者或本发明数据处理设备的记录和再现设备 300 与记录设备 400 之间执行密码翻译通信、相互鉴别、MAC 生成、验证等时，这些实体通常持有它们所共用的保密信息例如密钥信息。此外，在一个上多个实体之间例如在一个内容提供者与多个内容用户一个记录和再现设备与多个记录介质之间执行上述过程时，这些实体通常存储并持有所有实体所共用的保密信息即多个内容用户或多个记录介质所共用的密钥信息，或者，一个内容提供者单独管理并使用于各内容用户的保密信息(例如密钥)。

但是，就上述一对多的关系而言，拥有所有实体所共享的保密信息(密钥)的结构在下述方面是有缺陷的：从一个实体中泄露秘密会影响到使用同一保密信息(例如密钥)的所有其它实体。再有，在一个管理者例如内容提供者单独管理并使用用于各内容用户的保密记录和再现设备时，需要有一个列表，它用于标识所有的用户并将标识数据与独有的保密信息(例如密钥)联系起来，从而以与用户数成比例地最佳地增加列表维护和管理负担。

本发明的数据处理设备已利用用于保存主密钥并根据主密钥生成多种个别密钥的结构解决了在实体之间共享保密信息的这种通常问题。以下说明这种结构。

在本发明的数据处理设备中，如果记录设备即存储有内容的介质或记录和再现设备之间的各密码翻译处理、鉴别过程和类似过程等需要不同的个别密钥，则用诸如设备或介质所独有的标识数据(ID)之类的个别信息以及先前在记录和再现设备 300 中确定的个别密钥生成方法来生成这些个别密钥。利用这种结构，如果要识别出所生成的任一个别密钥，则可通过防止泄露相应的主密钥来排除对整个系统的破坏。此外，根据主密钥生成密钥的结构可消除对关联列表的需要。

以下参照附图说明结构的具体实例。图 49 是用于说说用记录和再

现设备 300 所持有多种主密钥来生成多种密钥的结构的图。图 49 中介质 500 和通信装置 600 如在前述实施例中那样输入内容。内容由内容密钥 Kcon 来加密，而内容密钥 Kcon 则是由发布密钥 Kdis 来加密的。

例如，如果记录和再现设备 300 试图从介质 500 或通信装置 600 中取出内容并将其下载至记录设备 400，则记录和再现设备 300 必须获得如前在图 2 和 39 至 41 中所述那样对内容密钥进行加密的发布密钥 Kdis。尽管密钥 Kdis 可从介质 500 和通信装置 600 中直接获得，或者，记录和再现设备 300 可事先获得该密钥并将其存储到存储器内。但是，用于将这种密钥发布给多种用户的结构会有泄露，这就会影响整个系统，如前所述。

本发明的数据处理系统配置成通过应用用于存储在记录和再现设备 300 的存储器中的发布密钥的主密钥 MKdis 并通过根据内容 ID 的过程即图 49 下部所示的 Kdis=DES(MKdis，内容 ID)生成发布密钥 Kdis。在从介质 500 或通信装置 600 中提供内容的内容提供者与是内容用户的记录和再现设备 300 之间的内容发布结构中，尽管有大量的内容提供者，但这种结构也能在不需要通过介质、通信装置或类似装置发布个别发布密钥 Kdis 或在不需要将它们存储在各记录和再现设备 300 的情况下保持先进的保密性。

以下说明鉴别密钥 Kakae 的生成。在如图 22 和 39 或 41 所述那样将内容从记录和再现设备 300 下载至记录介质 400 或如图 42 至 45 所述那样使记录和再现设备 300 执行并再现存储在记录介质 400 中的内容时，记录和再现设备 300 和记录介质 400 必须执行相互鉴别过程(见图 20)。

如图 20 所述，这种鉴别过程需要记录和再现设备 300 具有鉴别密钥 Kake。尽管记录和再现设备 300 可直接从例如记录介质 400 中获得鉴别密钥或事先获得并存储鉴别密钥，但用于将这种密钥发布给多种用户的结构会有泄露，这就会影响整个系统，如前在用于发布密钥的结构中所述。

本发明的数据处理系统配置成通过应用用于存储在记录和再现设备 300 的存储器中的发布密钥的主密钥 MKake 并通过根据记录设备 ID: IDmem 的过程即图 49 下部所示的 Kake=DES(MKake，IDmem)生成鉴别密钥 Kake。

此外，在如图 22 和 39 或 41 所述那样将内容从记录和再现设备 300 下载至记录介质 400 或如图 28、图 42 至 45 所述那样使记录和再现设备 300 执行并再现存储在记录介质 400 中的内容时，如果内容仅由特定的记录和再现设备所使用，则与用于上述发布或鉴别密钥相类的结构可用于生成记录和再现设备所独有的整体性检查值 ICVdev 所需的记录和再现设备签名密钥 Kdev。在上述实施例中，记录和再现设备签名密钥 Kdev 存储器在内部存储器中，但是，如果用于记录和再现设备签名密钥的主密钥 MKdev 存储在存储器中而记录和再现设备签名密钥 Kdev 不存储在存储器中，并且，如果记录和再现设备签名密钥 Kdev 如图 49 下部所示那样是通过 Kdes=DES(MKdev, IDdev)根据记录和再现设备标识符 IDdev 和用于记录和再现设备签名密钥的主密钥 MKdev 按需生成的，那么，对各设备来说，最好不必具有记录和再现设备签名密钥 Kdev。

通过这种方式，本发明的数据处理设备配置成根据主密钥和各 ID 生成诸如密钥之类在提供者与记录和再现设备或记录和再现设备与记录设备等两个实体之间的密码翻译信息处理所需的信息。因此，即使密钥信息从各实体中泄露，个别密钥所招致的破坏范围也是有限的，并且，如上所述，对个别实体来说也不必去管理密钥列表。

通过显示流程来说明与这种配置有关的过程的多个实例。图 50 示出内容产生者或管理者执行的用于用主密钥对内容等进行解密的过程以及用户设备例如上述加密中的记录和再现设备 300 执行用于用主密钥对加密的数据进行解密的过程的实例。

在步骤 S501 中，技术内容产生者或管理者将标识符(内容标识符)赋给内容。在步骤 S502 中，内容产生者或管理者根据所拥有的主密钥和内容 ID 生成密钥，以便对内容等加密。在这一步骤中，如果要生成发布密钥 Kdis，则根据上述 Kdis=DES(MKdis，介质 ID)来生成发布密钥 Kdis。然后，在步骤 S503 中，内容产生者或管理者用密钥(例如发布密钥 Kdis)对存储在介质中的部分或全部内容进行加密。内容产生者借助诸如 DVD、通信装置或类似装置提供通过这些步骤加密的内容。

另一方面，在步骤 S504 中，诸如记录和再现设备 300 之类的用户设备从经过诸如 DVD、通信装置或类似装置接收的内容数据中读出内容 ID。然后，在步骤 S505 中，用户设备根据读出的介质 ID 及其拥有的

主密钥生成密钥，它用于对加密的内容进行解密。如果要获得发布密钥 Kdis，则这种生成过程对应于例如发布密钥 Kdis=DES(MKdis，介质 ID)。在步骤 S506 中，用户设备用密钥对内容进行解密，并且在步骤 S507 中使用即再现解密的内容或执行程序。

在本例如，如图 50 的下部所示，内容产生者或管理者和用户设备均使主密钥(例如发布密钥生成主密钥 MKdis) 根据它们所拥有的主密钥和各 ID(介质 ID)顺序地生成对内容加密或解密所需的发布密钥。

利用这种系统，如果将发布密钥泄露给第三方，则第三方可对内容解密，但可防止对存储在其它介质中的有不同内容 ID 的内容解密，从而能使整个系统上泄露一个内容密钥的负面效果减至最少。另外，上述系统不需要用户设备即记录和再现设备去保存与用于各介质的列表相关联的密钥。

参照图 52 说明这样的实例，其中，内容产生者或管理者保存有多个主密钥以便根据内容发布目的地执行处理过程。

内容产生者或管理者执行的步骤 S511 包括将标识符(内容 ID)赋给内容。步骤 S512 包括选择内容产生者或管理者所持有的多个主密钥(例如多个发布密钥生成主密钥 Mkdis) 中的一个。尽管将参照图 52 作详细说明，但这一选择过程包括事先为内容所属的各个国家、各的类型或各设备版本设置应用主密钥并根据设置执行主密钥。

然后，在步骤 S513 中，内容产生者或管理者根据在步骤 S512 中选择的主密钥和在步骤 S511 中确定的内容 ID 生成加密密钥。如果例如要生成发布密钥 Kdis，则根据发布密钥 Kdis=DES(MKdis，介质 ID)生成该密钥。在步骤 S514 中，内容产生者或管理者用密钥(例如发布密钥 Kdis)对存储在介质上的部分或全部内容进行加密。在步骤 S515 中，内容产生者通过诸如 DVD、通信装置或类似装置之类的前质用发布单元来发布加密的内容，所述发布单元包括内容 ID、所使用的主密钥生成信息和加密的内容。

另一方面，在步骤 S516 中，例如诸如记录和再现设备 300 之类的用户设备判断它是否持有与诸如 DVD 之类介质或通信装置所发布的内容数据中的主密钥 ID 相对应的主密钥。如果不具有与内容数据中的主密钥 ID 相对应的主密钥，则该用户不能使用发布的内容，处理过程结束。

如果用户设备具有与内容数据中的主密钥 ID 相对应的主密钥，则在步骤 S517 从经介质、通信装置或类似装置接收的内容数据中读出内容 ID。然后，在步骤 S518 中，用户设备根据读出的内容 ID 和它持有的主密钥生成用于对加密内容进行解密的密钥。如果要获得发布密钥 Kdis，则这一过程是发布密钥 Kdisi=DES(MKdisi，内容 ID)。在步骤 S519 中，用密钥对内容进行解密。在步骤 S520 中，使用解密的内容，即进行再现或执行程序。

在本例中，如图 51 下部所示，内容产生者或管理者具有一主密钥集合，它包括多个主密钥例如发布密钥生成主密钥 MKdis1 至 N。另一方面，用户设备具有一个主密钥例如发布密钥生成主密钥 KKdisi，因此，个又在内容产生者或管理者使用了用于加密的 KKdisi 时才可对内容解密。

作为图 51 流程所示方面的具体实例，图 52 示出了这样一个实例，其中，应用了随国家而变的主密钥。内容提供者具有主密钥 MK1 至 n，其中，MK1 用生成这样的密钥，它们用于对发布给日本用户设备的内容进行加密。例如，根据内容 ID 和密钥 MK1 生成加密密钥 K1，然后用户对内容加密。主密钥 MK1 至 n 还设置成密钥 MK2 用于这样的密钥，它们用于对发布给美国用户设备的内容进行加密，密钥 MK3 用于这样的密钥，它们用于对发布给 EU(欧洲)用户设备的内容进行加密，

另一方面，就日本的用户设备具体说是在日本出售的诸如 PC 或游戏设备之类的记录和再现设备而言，主密钥 MK1 存储在其内部存储器中，就美国的用户设备而言，主密钥 MK2 存储在其内部存储器中，就 EU 的用户设备而言，主密钥 MK3 存储在其内部存储器中。

利用这种结构，内容提供者根据可以使用内容的用户设备有选择地使用主密钥 MK1 至 n 之一，以便对要发布给用户设备的内容加密。例如，为了使内容仅由日本的用户设备使用，将用主密钥 MK1 生成的主密钥 K1 用于对内容加密。加密的内容可用存储在日本用户设备中的主密钥 MK1 来解密，也就是说，允许生成解密密钥，而密钥 K1 不能分别从存储在美国和 EU 用户设备内的主密钥 MK2 和 MK3 中获得，从而能防止对加密的内容进行解密。

通过这种方式，内容提供者可有选择地用多个主密钥来设定用于多种内容的本地化。图 52 示出了这样的实例，其中，将不同的主密钥

用于用户设备所属的不同国家，但可以有多种使用形式，例如可根据用户设备的类型、版本切换主密钥，如上所述。

图 53 示出了这样的处理过程实例，其中，介质所独有的标识符即介质 ID 和主密钥结合在一起。这里，介质例如是指其中存储有内容的 DVD 或 CD。介质 ID 可为个别介质诸如电影之类的内容的名称或个别介质生产厂所独有。通过这种方式，可按多种方式分配介质 ID。

在步骤 S52 中，介质产生者或管理者确定用于介质的标识符(介质标识符)。在步骤 S522 中，介质产生者或管理者根据所拥有的主密钥和介质 ID 生成用于对存储在介质的内容进行加密的主密钥。在这一步骤中，如果要例如生成发布密钥 Kdis，则根据上述 Kdis=DES(MKdis，介质 ID)来生成发布密钥 Kdis。然后，在步骤 S523 中，介质产生者或管理者用密钥(例如发布密钥 Kdis)对存储在介质中的部分或全部内容进行加密。介质产生者提供通过这些步骤加密的内容。

另一方面，在步骤 S524 中，诸如记录和再现设备 300 之类的用户设备从所提供的介质中读出介质 ID。然后，在步骤 S525 中，用户设备根据读出的介质 ID 及其拥有的主密钥生成密钥，它用于对加密的内容进行解密。如果要获得发布密钥 Kdis，则这种生成过程对应于例如发布密钥 Kdis=DES(MKdis，介质 ID)。在步骤 S526 中，用户设备用密钥对内容进行解密，并且在步骤 S527 中再现解密的内容或执行程序。

在本例中，如图 53 的下部所示，介质产生者或管理者和用户设备均使主密钥(例如发布密钥生成主密钥 MKdis) 根据它们所拥有的主密钥和各 ID(介质 ID)顺序地生成对内容加密或解密所需的发布密钥。

利用这种系统，如果将介质密钥泄露给第三方，则第三方可对介质中的内容解密，但可防止对存储在其它介质中的有不同介质 ID 的内容解密，从而能使整个系统上泄露一个介质密钥的负面效果减至最少。另外，上述系统不需要用户设备即记录和再现设备去保存与用于各介质的列表相关联的密钥。再有，用一个介质密钥加密的内容的长度限于这样的量，它可存储在介质内，因此，内容不可能达到攻击加密文本所需的信息量，从而减少了对加密文本进行解密的可能性。

图 54 示出了这样的过程实例，其中，记录和再现设备所独有的标识符即记录和再现设备 ID 和主密钥结合在一起。

在步骤 S531 中，记录和再现设备的用户根据所主密钥和例如存储在记录和再现设备的内部存储器中的记录和再现设备 ID 生成用于对内容等进行加密的密钥。如果要例如获得内容密钥 Kcon，则这一生成过程对应用 Kcon=DES(MKcon，记录和再现设备 ID)。然后，在步骤 S532 中，用户用密钥(例如发布密钥 Kcon)对内容解密。在步骤 S533，用户将加密的内容存入诸如硬盘之类的记录和再现设备。

另一方面，当已存储内容的记录和再现设备用户请求恢复所存储的数据时，用于管理记录和再现设备的系统管理者从记录和再现设备中读出记录和再现设备 ID。然后，在步骤 S535 中，系统管理者根据读出的记录和再现设备 ID 及其拥有的主密钥生成密钥，它用于恢复加密的内容。如果要获得内容密钥 Kcon，则这种生成过程对应于例如内容密钥 Kcon=DES(MKcon，记录和再现设备 ID)。在步骤 S536 中，用户设备用密钥对内容进行解密。

在本例中，如图 54 的下部所示，记录和再现设备用户和系统管理者均使主密钥(例如内容密钥生成主密钥 MKcon) 根据它们所拥有的主密钥和各 ID(记录和再现设备 ID)顺序地生成对内容加密或解密所需的发布密钥。

利用这种系统，如果将内容密钥泄露给第三方，则第三方可对介质中的内容解密，但可防止对存储在其它介质中的有不同记录和再现设备 ID 的内容解密，从而能使整个系统上泄露一个内容密钥的负面效果减至最少。另外，上述系统不需要系统管理者或用户设备去保存与用于各介质的列表相关联的密钥。

图 55 示出了这样的结构，其中，根据主密钥生成从设备例如诸如存储卡之类的记录和再现设备与主设备例如记录和再现设备之间相互鉴别过程所使用的鉴别密钥。尽管在前述鉴别过程(见图 20)中鉴别密钥事先存储在从设备的内部存储器中，但也可在鉴别过程中根据主密钥生成鉴别密钥，如图 55 所示。

例如，在步骤 S541 中，作为在鉴别过程开始之前的初始化过程，是记录设备的从设备根据存储在是记录设备的从设备的内部存储器中主密钥和从设备 ID 生成供相互鉴别过程使用的鉴别密钥 Kake。鉴别密钥是 Kake=DES(MKake，从设备 ID)生成的。然后，在步骤 S542 中，将所生成的鉴别密钥存储在存储器内。

另一方面，诸如记录和再现设备之类的主设备通过通信装置从安装好的记录设备即从设备中读出从设备 ID。然后，在步骤 S544 中，主设备根据读出的从设备 ID 及其拥有的鉴别密钥生成主密钥生成鉴别密钥，它用于相互鉴别过程。这种生成过程对应于例如鉴别密钥 Kake=DES(MKake，从设备 ID)。在步骤 S545 中，鉴别密钥用于执行鉴别过程。

在本例中，如图 55 的下部所示，从设备和主设备均使是鉴别密钥生成立密钥 MKake 的根据它们所拥有的主密钥和从设备 ID 顺序地生成对鉴别过程所需的发布密钥。

利用这种系统，如果将鉴别密钥泄露给第三方，这种鉴别密钥仅对相应的从设备有效，而不能与其它从设备形成鉴别。从而能使泄露密钥的负面效果减至最少。

如上所述，本发明的数据处理设备配置成能生成诸如密钥之类在内容提供者与记录和再现设备或记录和再现设备与记录设备等两个实体之间的密码翻译信息处理所需的信息。因此，即使密钥信息从各实体中泄露，个别密钥所招致的破坏范围也是有限的，并且，如上所述，对个别实体来说也不必去管理密钥列表。

(13)在密码翻译处理过程中控制密码翻译处理的程度

在上述实施例中，用以参照图 7 所述的单 DES 结构为基础密码翻译处理过程连同实例主要说明了记录和再现设备 300 与记录设备 400 之间的密码翻译处理过程。用于本发明数据处理设备的加密处理方法并不局限于上述单 DES，而是可以根据所需的保密状态使用任何的加密方法。

例如，可以应用如图 8 至 10 所示的三重 DES 方法。例如，可将图 3 所示的记录和再现设备 300 的密码翻译处理部 302 及记录设备 400 的密码翻译处理部 401 配置成能执行三重 DES，因此，可根据图 8 至 10 所述的三重 DES 执行与密码翻译处理过程相对应的过程。

但是，内容提供者可根据内容将最高优先权给予处理速度，以便根据单 DES 方法使用 64 位内容密钥 Kcon，或者，将最高优先权给予保密性，以便根据根据三重 DES 方法使用 128 或 112 位内容密钥 Kcon。因此，将记录和再现设备 300 的密码翻译处理部 302 及记录设备 400 的密码翻译处理部 401 配置成仅包容三重 DES 和单 DES 方法中的一个

并不是最佳的。所以，记录和再现设备 300 的密码翻译处理部 302 及记录设备 400 的密码翻译处理部 401 应配置成能包含三重 DES 和单 DES 方法。

但是，为了将记录和再现设备 300 的密码翻译处理部 302 及记录设备 400 的密码翻译处理部 401 配置成能执行三重和单 DES 方法，必须为这些密码翻译处理部配备不同的电路和逻辑，以便使记录设备 400 执行与三重 DES 相对应的过程，必须将用于三重 DES 的命令集存储在图 29 所示的命令寄存器内。这就会使记录设备 400 中的处理部变得复杂。

因此，就本发明的数据处理设备而言，提出了这样一种结构，其中，记录设备 400 的密码翻译处理部 401 的逻辑配置成包容单 DES，同时能执行与三重 DES 过程相对应的处理过程，以便将根据三重 DES 方法加密的数据(密钥、内容或类似数据)存储进记录设备的外部存储器 402。

例如，在图 32 所示的用于数据格式类型 0 的实例中，当将内容数据从记录和再现设备 300 中下载至记录设备 400 时，在示出了下载格式类型 0 的数据的图 39 所述的步骤 S101 中执行鉴别过程，并且，生成会话密钥 Kses。再有，在步骤 S117 中，记录和再现设备 300 的密码翻译处理部 302 用会话密钥 Kses 对内容密钥 Kcon 进行加密并通过通信装置将加密的密钥传给记录设备 400。在步骤 S118 中，已接收到加密的密钥的记录设备 400 的密码翻译处理部 403 会话密钥 Kses 对内容进行解密，并用存储密钥 Kstr 对数据加密，且将最终的密钥传给记录和再现设备 300 的密码翻译处理部 302。记录和再现设备 300 顺序地形成数据(步骤 S1217 并将带格式的数据传给记录设备 400，而且，记录设备 400 将接收到的数据存储到外部存储器 402 中。

如果将记录设备 400 的密码翻译处理部 401 在上述过程的步骤 S117 与 S118 之间执行的密码翻译处理过程配置成有选择地执行单或三重 DES 方法，则密码翻译处理部检查内容提供者按三重 DES 还是按单 DES 用内容密钥 Kcon 提供内容数据。

图 56 示出了用于说明用记录和再现设备 300 的密码翻译处理部 302 和记录设备 400 的密码翻译处理部 401 执行符合三重 DES 方法的密码翻译处理方法的结构的流程。图 56 示出了用于用存储密钥 Kstr 对

内容密钥 Kcon 进行加密的过程的实例，所述过程是在将内容数据从记录和再现设备 300 中下载至记录设备 400 时进行的，其中，内容密钥 Kcon 是以三重 DES 方法为基础。这里，示出了用于内容密钥 Kcon 的过程的实例，其它密钥或诸如内容之类的其它数据是以类似方式处理的。

三重 DES 方法按下述方式使用了两个或三个密钥即：64 位密钥用于单 DES，而 128 位密钥用于三重 DES，如前在图 8 至 10 中所述。这三个内容密钥 Kcon 是指 Kcon1、Kcon2 和(Kcon3)。在括号中示出了 Kcon3，因为，Kcon3 可能未使用。

以下说明图 56 中的过程。在步骤 301 中，在记录和再现设备 300 与记录设备 400 之间进行相互鉴别处理。在先前图 20 所述的过程中执行这种相互鉴别处理。在这种鉴别过程中，生成会话密钥 Kses。

一旦完成了步骤 S301 中的鉴别过程，就比较包括整体性检查值 A 和 B、内容整体性检查值和总体整体性检查值在内的整体性检查值 ICV。

当比较了所有的检查值(ICV)且判断出没有数据被篡改，处理过程就前进至步骤 S303，在步骤 S303 中，记录和再现设备 300 的记录和再现设备密码翻译处理部 302 的控制部 306 用记录和再现设备密码翻译处理部 302 的加密/解密部 308 以及先前获得或生成的发布密钥 Kdis 存储在数据的头标部中的内容 Kcon 进行解密，所述数据是从介质 500 获得的或者是通过通信部 305 从通信装置 600 中接收的。内容密钥在这种情况下是诸内容密钥 Kcon1、Kcon2 和(Kcon3)之类的三重 DES 类型的密钥。

在步骤 S304 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 用在相互鉴别过程中可共享的会话密钥 Kses 仅对内容密钥 Kcon1、Kcon2 和(Kcon3)中的内容密钥 Kcon1 进行加密。

记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读出数据，该数据包含有用会话密钥 Kses 加密的密钥密钥 Kcon1。控制部 301 然后将这些数据通过记录和再现设备 300 的记录设备控制器 303 传给记录设备 400。

然后，在接收到传送自记录和再现设备 300 的内容密钥 Kcon1 时，

记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用在相互鉴别过程中可共享的会话密钥 Kses 对接收到的内容密钥 Kcon1 进行解密。此外，在步骤 S306 中，记录设备 400 使加密/解密部 406 用存储在记录设备密码翻译处理部的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对解密的内容密钥进行重新加密，并将重加密的密钥通过通信部 404 传给记录和再现设备 300。

在步骤 S307 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 用在相互鉴别过程中可共享的会话密钥 Kses 仅对在步骤 S303 中解密的内容密钥 Kcon1、Kcon2 和(Kcon3)中的内容密钥 Kcon2 进行加密。

记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读出数据，该数据包含有用会话密钥 Kses 加密的密钥密钥 Kcon2。控制部 301 然后将这些数据通过记录和再现设备 300 的记录设备控制器 303 传给记录设备 400。

在步骤 308 中，在接收到传送自记录和再现设备 300 的内容密钥 Kconz 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用在相互鉴别过程中可共享的会话密钥 Kses 对接收到的内容密钥 Kcon2 进行解密。此外，在步骤 S309 中，记录设备 400 使加密/解密部 406 用存储在记录设备密码翻译处理部的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对解密的内容密钥进行重新加密，并将重加密的密钥通过通信部 404 传给记录和再现设备 300。

然后，在步骤 S310 中，记录和再现设备密码翻译处理部 302 的控制部 306 使记录和再现设备密码翻译处理部 302 的加密/解密部 308 用在相互鉴别过程中可共享的会话密钥 Kses 仅对在步骤 S303 中解密的内容密钥 Kcon1、Kcon2 和(Kcon3)中的内容密钥 Kcon3 进行加密。

记录和再现设备 300 的控制部 301 从记录和再现设备 300 的记录和再现设备密码翻译处理部 302 中读出数据，该数据包含有用会话密钥 Kses 加密的密钥密钥 Kcon3。控制部 301 然后将这些数据通过记录和再现设备 300 的记录设备控制器 303 传给记录设备 400。

然后，在步骤 S311 中，在接收到传送自记录和再现设备 300 的内容密钥 Kcon3 时，记录设备 400 就使记录设备密码翻译处理部 401 的加密/解密部 406 用在相互鉴别过程中可共享的会话密钥 Kses 对接收

到的内容密钥 Kcon3 进行解密。此外，在步骤 S312 中，记录设备 400 使加密/解密部 406 用存储在记录设备密码翻译处理部的内部存储器 405 内的为记录设备所独有的存储密钥 Kstr 对解密的内容密钥进行重新加密，并将重加密的密钥通过通信部 404 传给记录和再现设备 300。

然后，在步骤 S313 中，记录和再现设备的密码翻译处理部构成了图 32 至 35 所述的多种数据格式并将它们传给记录设备 400。

最后，在步骤 S314 中，记录设备 400 将接收到的带格式的数据存储到外部存储器 402 内。这些格式数据包含用存储密钥 Kstr 加密的内容密钥 Kcon1、Kcon2 和(Kcon3)。

上述过程能根据三重 DES 密码系统将存储在记录设备 400 中的内容密钥存储为密钥。如果仅使用两个内容密钥 Kcon1 和 Kcon2，则略去从步骤 S310 至 S312 的处理过程。

如上所述，记录设备 400 可通过在仅有目标产生变化的情况下重复同样方面的处理过程即步骤 S305 和步骤 S306 中的处理步骤多次将带有应用给它的三重 DES 的密钥存储在存储器内。如果将单 DES 应用给内容密钥 Kcon，则可执行步骤 S305 和 S306，以便在将密钥存储到存储器中之前执行步骤 S313 中的格式化过程。这种结构可将用于执行步骤 S305 和 S306 中处理过程的命令存储到先前图 29 所述的命令寄存器中并根据密钥的方面即密钥是基于三重还是单 DES 方法执行上述处理过程一至三次。因此，可在记录设备 400 的处理逻辑中不包含三重 DES 处理方法的情况下执行基于三重和单 DES 方法的过程。这方面，密码系统可记录在内容数据的头标部中的使用策略内，以便通过引用使用策略来加确定。

(14)基于内容数据使用策略中启动优先权的程序启动过程

从图 4 至 6 所述的内容数据结构中可以看出，存储在本发明数据处理设备所使用的内容数据头标部中的使用策略包含内容类型和启动优先权。就记录在诸如记录设备 400、DVD、CD、硬盘或游戏盒之类多种记录介质中的多种可访问的内容数据而言，本发明数据处理设备中的记录和再现设备 300 可依照启动优先权确定启动这些内容的次序。

记录和再现设备 300 执行与诸如各记录设备 DVD 设备、CD 驱动设备和硬盘驱动设备之类的多种记录设备的相互鉴别，然后，依照内容数据中的优先权按最高优先权执行内容数据中的程序。以下说明“基

于内容数据使用策略中启动优先权的程序启动过程”

如果记录和再现设备 300 再现并执行来自一个记录设备 400 的内容数据，则本发明数据处理设备的上述说明侧重于所执行的处理过程。但是，记录和再现设备 300 一般配置成除记录设备 400 以外还能通过读取部 304 访问 DVD、CD 和硬盘以及诸如存储卡和游戏盒之类的通过 PIO111 或 STO112 连接的记录介质。在图 2 中，仅说明了一个读取部，以避免使图复杂化，记录和再现设备 300 可具有不同的记录介质例如 DVD、CD、软盘和硬盘，它们并行地安装在记录和再现设备内。

记录和再现设备 300 可访问多个记录介质，每个记录介质均存储有内容数据。诸如 CD 之类外部内容提供者所提供的内容数据按图 4 所示的数据结构存储在介质内或者在数据是从介质中取出的或通过通信装置下载的情况下按图 26 或 27 所示的内容数据结构存储在诸如存储卡之类的各记录介质内。此外，具体地说，内容数据根据其格式类型按不同的格式存储在介质和记录设备上，如图 32 至 35 所示。在这种情况下，内容数据的头标中的使用策略包含内容类型和启动优先权。

依照上述流程说明在可访问多个内容数据的情况下的由记录和再现设备所执行的用于启动内容的过程。

图 57 示出了这样的流程，它示出了存在有可以启动的多个内容数据的过程的实例(1)。在步骤 S611 中，鉴别可由记录和再现设备 300 所访问的记录设备。可访问的记录设备包括存储卡、DVD 设备、CD 驱动器、硬盘设备和游戏盒或例如通过 PIO111 或 SIO112 连接的类似设备。在图 2 所示的控制部 301 的控制下例如按先前图 20 所述的过程鉴别各记录设备。

在步骤 S612 中，从存储在成功鉴别的记录设备的存储器中内容数据检测可启动的程序。具体地说，这一过程是作为抽取内容的过程来执行的，就所述内容而言，包含在内容数据的使用策略中的内容类型表示是程序。

在步骤 S613 中，确定可启动的且已在步骤 S612 中抽取出来的程序的优先权。具体地说，这个过程对应于比较包含在可于步骤 S612 中启动的多个内容数据的头标内使用策略中的优先权，以便选定最高优先权。

然后，在步骤 S614 中，启动选定的程序。如果可启动的多个程序

具有同样的优先权，则为记录设备设置缺省的优先权，因此，可执行存储在设备中有最高优先权的内容程序。

图 58 示出了处理过程即用于可启动的多个内容的过程的实例(2)，其中，为多个记录设备设置标识符，因此，就带有标识符的记录设备而言可顺序地鉴别和检索内容程序。

在步骤 S621 中，鉴别安装在记录和再现设备 300 中的记录设备(i)。将标识符 1 至 n 顺序地赋给(n)个记录设备 400。

在步骤 S622 中，判断步骤 S621 中的鉴别是否成功，如果是，则处理过程前进至步骤 S623，在该步骤中，从记录设备(i)的记录介质中检索出可启动的程序。如果鉴别失败，则处理过程前进至步骤 S627，在该步骤中，判断是否存在有从中检索出内容的新记录设备。在没有这种记录设备的情况下，结束处理过程，否则，处理过程前进至步骤 S628 以更新记录设备标识符并重复步骤 S621 和随后的鉴别处理步骤。

在步骤 S623 中，从存储在记录设备(i)内的内容数据中检测可启动的程序。具体地说，这一过程是作为抽取内容的过程来执行的，就所述内容而言，包含在内容数据的使用策略中的内容类型表示是程序。

在步骤 S624 中，判断是否抽取了其内容类型是程序的内容。如果已抽取了内容，则在步骤 S626 中选定抽出的具有最高优先权的程序。

如果在步骤 S624 中判断未抽出内容类型是程序的内容，则处理过程前进至步骤 S627 以判断是否存在有从中检索出内容的新记录设备。在没有这种记录设备的情况下，结束处理过程，否则，处理过程前进至步骤 S628 以更新记录设备标识符 i 并重复步骤 S621 和随后的鉴别处理步骤。

图 59 示出了一流程，该流程示出了用于可启动的多个内容的过程的实例。在步骤 S651 中，对可由记录和再现设备 300 访问的记录设备进行鉴别。鉴别可访问的 DVD 设备、CD 驱动器、硬盘设备和游戏盒或类似设备。在图 2 所示的控制部 301 的控制下例如按先前图 20 所述的过程鉴别各记录设备。

在步骤 S652 中，从存储在成功鉴别的记录设备的存储器内的内容数据中检测可启动的程序。具体地说，这一过程是作为抽取内容的过

程来执行的，就所述内容而言，包含在内容数据的使用策略中的内容类型表示是程序。

然后，在步骤 S653 中，将诸如可启动的程序的名字之类的业已在步骤 S652 中抽出的信息显示到显示装置上。尽管在图 2 中未示出显示装置，但可将 AV 输出数据输出给显示装置(未示出)。诸如用于各内容数据的程序名之类的用户提供的信息存储在内容数据的内容 ID 中，因此，诸如用于各已鉴别的内容数据的程序名之类的程序信息可通过控制部 301 在图 2 所示的主 CPU106 的控制下输出给输出装置。

在步骤 S654 中，主 CPU106 通过接口 10 从诸如输入接口、控制器、鼠标或键盘中接收用户的程序选择输入，在步骤 S655 中，根据选择输入启动用户选定的程序。

如前所述，在本发明的数据处理设备中，程序启动优先权存储在内容数据的头标的使用策略中，因此，记录和再现设备 300 可根据优先权启动程序，或者，显示装置显示用户可从中选择预定程序的启动信息。这种结构消除了用于检索程序的需要，从而节约了时间和启动所需的劳动力。此外，在所有的记录设备都已鉴别或显示出是这样的程序之后启动可启动的程序，从而消除了诸如需要在选择之后确认过程之类的处理过程的复杂性。

(15) 内容结构和再现(解压缩)过程

在本发明的数据处理设备中，记录和再现设备 300 从介质 500 或通信装置 600 中下载内容或再现来自记录设备 400 的数据，如前所述。上述说明侧重于与内容的下载或再现有关的加密数据处理过程。

图 3 中记录和再现设备 300 的控制部 301 一般控制着与从诸如 DVD 之类提供内容数据的设备 500、通信装置 600 或记录设备中下载或再现有关的鉴别、加密和解密过程。

源于这些过程的可再现内容例如是声音或图像数据或类似数据。来自控制部 301 的解密数据置于图 2 所示的主 CPU 的控制之下并根据声音或图像数据或类似数据输出给 AV 输出部。但是，如果内容例如是经 MP3 压缩的声音数据，图 2 所示的 AV 输出部中的 MP3 解码器就对声音数据解密并加以输出。此外，如果内容数据是经 MPEG2 压缩的图像，AV 输出部中的 MP2 解码器就对图像数据解压缩并加以输出。通过这种方式，包含在内容数据中的数据可以或者不压缩(编码)并且在处理之

后根据内容加以输出。

但是，由于有多种类型的压缩和解压缩处理程序，所以，即使内容提供者提供压缩数据，则在没有相应解压缩处理执行程序情况下不能再现这些数据。

因此，本发明公开了这样一种数据处理设备，其中，压缩数据以及用于该数据的解密(解压缩)处理程序存储在数据内容，或者，用于压缩数据的链接信息以及用于该信息的解密(解压缩)处理程序存储为内容数据中的头标信息。

图 60 是从图 2 所示的数据处理的总体角度上简化与结构有关的部件所获得的图。记录和再现设备 300 从诸如 DVD 或 CD 之类的设备 500、通信装置 600、或诸如存储卡之类存储有内容的记录设备 400 中接收多种内容。这些内容包括诸如声音数据、静态图像、动画图像数据以及已被或未被加密或压缩的程序数据之类的多种数据。

如果已对接收到的内容加密，则用诸如上述方法之类的方法根据控制部 301 和密码翻译处理部 302 的密码翻译处理过程的控制执行解密过程。在 CPU106 的控制下将解密的数据传给 AV 处理部 109，其中，数据存储在 AV 处理部 109 的存储器 3090 内。然后，内容分析部 3091 分析内容的结构。如果例如数据压缩程序存储在内容中，则将该程序存储到程序存储部 3093 内。如果内容包含声音或图像数据或类似数据，则这些数据存储在数据存储部 3092 内。压缩和解压缩处理部 3094 用诸如 MP3 之类存储在程序存储部内的解压缩处理程序对存储在数据存储部 3092 中的压缩数据进行解压缩。然后，数据输出给扬声器 3001 或监视器。

以下说明 AV 处理部 109 通过控制部 301 接收的数据的结构和相关处理过程的某些实例。这里，将声音数据显示为内容的实例，并且，将应用了 MP3 的内容说明为代表性压缩数据。但是，这种结构也可应用于图像数据和声音数据，不仅可以应用 MP3 解压缩程序，而且可应用用于 MPEG2 或 MPEG4 的其它多种这样的程序。

图 61 示出了内容结构的一个实例。该图示出了通过 MP3 和 MP3 解密(解压缩)处理程序 6101 来压缩的音乐数据 6102，所述数据和程序一起综合成一个内容。这种内容均存储在介质 500 或记录设备 400 并且作为单一的内容发布自通信装置 600。如果这些内容如前所述那样业已

加密，则记录和再现设备 300 用密码翻译处理部 303 对内容解密并将其传给 AV 处理部 109。

AV 处理部 109d 内容分析部 3091 从包括声音数据解压缩程序(MP3 解码器)部和压缩声音数据部的内容中取出声音数据解压缩程序(MP3 解码器)部并将其存储到程序存储部 3093，同时将压缩的声音数据存储到数据存储部 3092。内容分析部 3091 除内容以外还可接收诸如内容名或内容结构信息之类的信息，或者根据包含在内容中的诸如数据名之类的标识数据或诸如数据长度或数据结构之类的其它数据对内容进行分析。然后，压缩和解压缩部 3094 根据存储在程序存储部 3093 中的声音数据解压缩程序(MP3 解码器)对存储在数据存储部 3092 中的 MP3 压缩声音数据进行解压缩。AV 处理部 109 然后将解压缩的声音数据输出给扬声器 3001。

图 62 示出了一流程图，它示出了用于再现图 61 内容结构的数据的过程的一个实例。在步骤 S671 中，如果内容是声音数据，则从独立接收自内容或接收自内容数据的信息中取出存储在 AV 处理部 101 的存储器 3090 中的数据名例如诸如音乐的标题之类的信息，并将其显示到监视器 3002 上。在步骤 S672 中，通过输入接口 110 从诸如开关和键盘之类的多种输入装置之一中接收用户选择，然后，在 CPU106 的控制下将基于用户输入数据的再现处理命令输出给 AV 处理部 109 。在步骤 S673 中，AV 处理部 109 抽出并对用户选择的数据并解压缩。

图 63 示出了结构实例，其中，内容包含压缩的声音数据或解压缩处理程序并且还将表示内容包含有什么的内容信息包含为用于各内容的头标信息。

如图 63 所示，如果内容是程序 6202，则内容包含作为头标信息 6201 的内容标识信息，它表示该内容是程序且程序的类型是对 MP3 解压缩的。另一方面，如果声音数据 6204 被包含为内容，则头标 6203 中的内容信息表示数据已经进行了 MP3 压缩。可通过仅选择从包含在例如图 4 所示上述内容数据结构的使用策略(见图 5)内的数据中进行再现所需的信息并将该信息附加给传给 AV 处理部 109 的内容，从而对上述头标信息进行配置。具体地说，将用于密码翻译处理部 302 所需的使用策略数据并用于 AV 处理部 109 在再现过程中所需的数据的标识值附加给图 5 所示的“使用策略”的各个构成数据，并且，仅将表示

这些标识值是 AV 处理部 109 所必需的数据抽取成头标信息。

一旦接收到了图 63 所示的各个内容，AV 处理部 109 的内容分析部 3091 就根据头标信息将程序内容在内容是程序的情况下存储到程序存储部 3093 或在内容是数据的情况下存储到数据存储部 3092。此后，压缩和解压缩部 3094 从数据存储部中取出数据并在输出解压缩数据之前根据存储在程序存储部 3093 中的 MP3 程序对数据解压缩。如果程序存储部 3093 具有已存储在其中的同样程序，则可略去程序存储过程。

图 64 示出了一流程，它示出了用于再现图 63 内容结构的数据的过程的一个实例。在步骤 S675 中，如果内容是声音数据，则从独立接收自内容或接收自内容头标的信息中取出存储在 AV 处理部 101 的存储器 3090 中的数据名（例如诸如音乐的标题之类的信息），并将其显示到监视器 3002 上。在步骤 S676 中，通过输入接口 110 从诸如开关和键盘之类的多种输入装置之一中接收用户选择。

然后，在步骤 S677 中，检索与用户选择相对应的内容再现程序(例如 MP3)。这种程序检索的最大范围最好设置为记录和再现设备 300 的可能访问范围，并且，例如，图 60 所示的介质 500、通信装置 600 和记录设备 400 均包括在检索范围内。

只有传给 AV 处理部 109 的内容是数据部，而程序内容则可存储在记录和再现设备 300 的另一个记录介质内或者是由内容提供者通过诸如 DVD 或 CD 之类介质提供的。因此，将检索范围设置成记录和再现设备 300 的可能检索范围。当作为检索结果找到再现程序时，在 CPU106 的控制下将基于用户输入数据的再现处理命令输出给 AV 处理部 109 。在步骤 S679 中，AV 处理部 109 根据用户的选择抽出数据并对数据解压缩。在另一个实施例中，在步骤 S675 之前执行程序检索，因此，在步骤 S675 中只会显示已检测到程序的数据。

图 65 示出了结构实例，其中，内容包含压缩的声音数据 6303 和解压缩处理程序 6302 并且还将内容再现优先权包含为用于内容的头标信息 6301。这是上述图 61 所示的内容结构的实例，带有作为头标信息增加给它的再现优先权。如在上述部分“(14) 基于内容数据使用策略中启动优先权的程序启动过程”中那样，根据 AV 处理部 109 所接收的内容之间设置的再现优先权确定再现次序。

图 66 示出了一流程，它示出了用于再现图 65 内容结构的数据的

过程的一个实例。在步骤 S681 中，将存储在 AV 处理部 109 的存储器 3090 中的数据即用于要加以再现的数据信息设置在检索列表中。用 AV 处理部 109 的存储器的某些区域来设置检索列表。然后，在步骤 S682 中，AV 处理部 109 的内容分析部 3091 选择最高优先权的数据，并且，在步骤 S683 中，再现选定的数据。

图 67 示出了结构实例，其中，内容包含头标信息和程序数据 6402 或头标信息 6403 和压缩数据 6404 的组合，并且，仅将再现优先权增加给数据内容的头标 6403。

图 68 示出了一流程，它示出了用于再现图 67 内容结构的数据的过程的一个实例。在步骤 S691 中，将存储在 AV 处理部 109 的存储器 3090 中的数据即用于要加以再现的数据信息设置在检索列表中。用 AV 处理部 109 的存储器的某些区域来设置检索列表。然后，在步骤 S692 中，AV 处理部 109 的内容分析部 3091 选择最高优先权的数据。

然后，在步骤 S693 中，检索与用户选择相对应的内容再现程序(例如 MP3)。如在图 64 的流程中那样，这种程序检索的最大范围最好设置为记录和再现设备 300 的可能访问范围，并且，例如，图 60 所示的介质 500、通信装置 600 和记录设备 400 均包括在检索范围内。

当作为检索结果找到再现程序时(步骤 S694 中的是)，用因检索所获得的程序对选定的数据进行解压缩并再现。

另一方面，如果作为检索结果未找到再现程序时(步骤 S694 中的是)，则处理过程前进至步骤 S696，以删除包含在于步骤 S691 设置的检索列表内的其余数据中必须用同一程序来再现的那些数据。这是因为，很明显，从这些数据中检索出再现程序的新的尝试是失败的。此外，当判断检索列表是否为空，并且，如果判断出该列表不为空，则处理过程返回至步骤 S692，以抽出下一个最高优先权的数据，从而执行程序检索过程。

因此，依照这种结构，如果压缩的内容是用其解密(解压缩)程序构成的或者仅包括通过使内容压缩而获得的数据或仅包括解压缩处理程序，那么，由于所述内容具有头标信息，它表示内容是什么压缩数据或内容执行什么过程，所以，接收内容的处理部(例如 AV 处理部)会使用与压缩数据相连的解压缩处理程序，以便执行解压缩或再现处理或根据压缩数据中的头标信息检索解压缩和再现程序，从而根据因检

索而获得的程序执行解压缩和再现。这就消除了对用户执行的诸如选择和检索数据解压缩程序的过程的需要，从而降低了用户的负担，因此能进行有效的数据再现。而且，头标中带有再现优先权的结构能自动地设置再现次序，从而使用户省去设置再现次序的操作。

在上述实施例中，MP3被看作是用于压缩的声音数据内容和声音压缩数据的解压缩处理程序的实例，但是，这种结构还可应用于包含压缩数据或压缩图像数据的解压缩处理程序的内容并且在这种情况下能提供相类似的效果。

(16)生成保存数据并将保存数据存储在记录设备内且再现来自记录设备的保存数据

例如，如果在记录和再现设备 300 中执行的内容是游戏程序或类似内容，并且，如果游戏程序要在挂起之后的预定时间继续，则游戏或类似内容在挂起时的状态要加以保存即存储在记录设备内，以便能够在继续时读出，从而使游戏继续进行。

在通常的用于游戏设备、个人计算机或类似设备的记录和再现设备中，保存数据保留结构配备有这样的结构以便将保存数据保留在能嵌入记录和再现设备或从外部与记录和再现设备相连的诸如存储卡、软盘、游戏盒或硬盘之类的记录介质内。但是，具体地说，这些记录和再现设备不具有用于保持保存数据保密性的结构，从而能用例如为游戏应用程序所共用的规范进行保存处理。

因此，例如，用记录和再现设备 A 所保存的保存数据可用于被其它游戏程序所重写；很少注意到保存数据的保密性。

本发明的数据处理设备提供了这样一种结构，它可保持保存数据的保密性。例如，可根据仅由某种游戏程序使用的信息在用于该游戏程序的保存数据存储到记录设备之前对该保存数据进行加密。另外，可根据记录和再现设备所独有的信息在保存数据存储到记录设备之前对该保存数据进行加密。这些方法可以使得保存数据的使用限于特定的设备或程序，以便保持数据的保密性。以下说明本发明数据处理设备中的“生成保存数据并将保存数据存储在记录设备内且再现来自记录设备的保存数据”

图 69 是用于说明本发明数据处理设备中保存数据存储过程的框图。将来自诸如 DVD 或 CD 之类介质 500 或通信装置 600 的内容提供给

记录和再现设备 300。所提供的内容已用内容密钥 Kcon 加密，内容密钥 Kcon 如上所述是内容所独有的密钥，并且，记录和再现设备 300 可根据“(7)用于从记录和再现设备下载至记录设备的过程”(见图 22)中所述的过程获得内容密钥，以便对加密的内容解密然后将其存储进记录设备 400。以下说明涉及记录和再现设备 300 执行的过程，该过程用于对来自介质或通信装置的内容程序解密、再现并执行上述程序、然后将所获得的保存数据存储在用于再现的诸如外部或内置存储卡和硬盘之类的多个记录设备 400A、400B 和 400C 之一中，或者，下载记录设备 400A 中的内容、再现并执行来自记录设备 400A 的内容、并将最终的保存数据存储到处理和记录设备 400 内以便将保存数据存储到用于再现的诸如外部或内置存储卡和硬盘之类的多个记录设备 400A、400B 和 400C 任何一个中并再现保存数据。

如前所述，记录和再现设备 300 具有：记录和再现设备标识符 IDdev；系统鉴名密钥 Ksys，它是整个系统共享的签名密钥；记录和再现设备签名密钥 Kdev，它是个别记录和再现设备所独有的；以及，主密钥，它用于生成多种个别密钥。如在“(12) 基于主密钥生成密码翻译处理过程密钥的结构”中所详述那样，主密钥用于生成例如发布密钥 KKdis 或鉴别密钥 Kake。这里，主密钥的类型没有具体限制，但用 MKx 来表示代表记录和再现设备 300 的主密钥的密钥。图 69 在下部示出了用于保存数据的密码翻译密钥 Ksav 的一个实例。

保存数据密码翻译密钥：Ksav=Kcon

保存数据密码翻译密钥：Ksav=Ksys

保存数据密码翻译密钥：Ksav=Kdev

保存数据密码翻译密钥：Ksav=内容 ID 或 DES（MKx，内容 ID）

保存数据密码翻译密钥：Ksav=记录和再现设备 ID（IDdev）或 DES（MKx，记录和再现设备 ID（IDdev））

保存数据密码翻译密钥：Ksav=（Kcon^Kdev）或 DES（MKx，Kcon^Kdev）

保存数据密码翻译密钥：Ksav=（内容 ID^Kdev）或 DES（MKx，内容 ID^Kdev）

保存数据密码翻译密钥：Ksav=(KCON^记录和再现设备 ID)或 DES（MKx，KCON^记录和再现设备 ID）

保存数据密码翻译密钥：Ksav=（内容 ID^记录和再现设备 ID）或 DES（MKx，内容 ID^记录和再现设备 ID）

保存数据密码翻译密钥：Ksav=口令或 DES（MKx，口令）等。

保存数据密码翻译密钥 Ksav 用于加密过程和解密过程，加密过程可进行执行以将保存数据存储在多个记录设备 400A 至 C 之一内，解密过程可进行执行以再现来自多个记录设备 400A 至 C 之一的保存数据。以下参照图 70 和后续附图说明存储和再现保存数据的过程。

图 70 是用内容独有的密钥或系统共用密钥将保存数据存储到记录设备 400A 至 C 之一中的过程的流程。每各流程中的过程均由记录和再现设备 300 来执行，将保存数据存储在各流程中的记录设备 400 可以是任何一种外部记录设备 400A 至 C 并且不限于具体的某一个。

在步骤 S701 中，记录和再现设备 300 读出内容 ID 例如游戏 ID。这种 ID 是包含在先前图 4、26、27 和 32 至 35 所示的内容数据的标识信息中的数据。在通过图 2 所示的接口接收到用于存储保存数据的命令时，主 CPU106 命令控制部 301 读取内容 ID。

如果执行程序是来自通过读取部 304 执行 DVD、CD-ROM 或类似装置的内容，则控制部 301 通过读取部从内容数据的头标中取出标识信息，如果执行程序是存储在记录设备 400 内的内容，则控制部 301 通过记录设备控制器 303 取出标识信息。如果记录和再现设备 300 正在执行内容程序且内容 ID 已存储在记录和再现设备的 RAM 或其它可访问记录介质中，则可在不执行新的读取程序的情况下使用包含在加载的数据中的标识信息。

在步骤 S702 中，根据程序是否本地化来改变处理过程。程序本地化用于设置是否增加仅由这一程序使用保存数据的限制、使保存数据仅由这一程序使用即 "程序本地化"置成 "是"、以及防止将数据的使用限于这一程序即程序本地化"置成 "否"。这一点可由用户来任意地设置或者可以由内容产生者来设置并存储到内容程序中，而且，将设置的本地化作为数据管理文件存储在图 69 的记录设备 400A 至 C 之一中。

图 71 示出了数据管理文件的一个实例。数据管理文件被生成为一个表，它包含有条目，条目包括数据号、内容 ID、记录和再现设备 ID 和程序本地化。内容 ID 是用于为其保存了保存数据的内容程序。记录

和再现设备 ID 表示已存储了保存数据的记录和再现设备，它的一个实例是图 69 所示的[IDdev]。程序本地化设置成“是”，以便使保存数据仅由这一程序使用，程序本地化设置成“否”，以便防止将数据的使用限于这一程序。程序本地化可由用户用内容程序来任意地设置或者可以由内容产生者来设置并存储到内容程序中。

参照图 70，继续说明流程。如果在步骤 S702 中将程序本地化置成“是”，则处理过程前进至步骤 S703。在步骤 S703 中，从内容数据中读出内容独有的密钥例如内容密钥 Kcon 并将其用作保存数据密码翻译密钥 Ksav，或者根据内容独有的密钥生成保存数据密码翻译密钥 Ksav。

另一方面，如果在步骤 S702 中将程序本地化置成“否”，则处理过程前进至步骤 S707。在步骤 S707 中，从记录和再现设备 300 的内部存储器 307 中读出存储在记录和再现设备 300 中的系统共用密钥例如系统签名密钥 Ksys 并将其用作保存数据密码翻译密钥 Ksav，或者，根据系统签名密钥 Ksys 生成保存数据密码翻译密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据密码翻译密钥 Ksav。

在步骤 S704 中，用在步骤 S703 或 S707 中选定或生成的保存数据密码翻译密钥 Ksav 执行对保存数据进行加密的过程。用图 2 的密码翻译处理部 302 通过应用例如上述 DES 算法来执行加密过程。

在步骤 S705 中，将在步骤 S704 中加密的保存数据存储在记录设备中。如果如图 69 所示存在有多个能存储保存数据的记录设备，则用户事先将记录设备 400A 至 C 选定为保存数据存储目的地。此外，在步骤 S706 中，将在步骤 S702 中设置程序本地化即程序本地化的“是”或“否”写至参照图 71 所述的数据管理文件。

因此，完成了用于存储保存数据的过程。在步骤 S702 中，可防止不具有内容独有密钥信息的内容程序对在步骤 S702 中程序本地化选定为“是”的并在步骤 S703 中用根据内容独有密钥生成的保存数据加密密钥 Ksav 来加以加密的保存数据进行解密，因此，这些保存数据仅能由具有相同内容密钥信息的内容程序来使用。但是，在这种情况下，保存数据加密密钥 Ksav 不是根据记录和再现设备所独有的信息生成的，因此，只要能同相应的内容程序一起使用，存储在诸如存储卡之

类可拆卸记录设备中的保存数据就可从不同的记录和再现设备中再现。

另外，即使使用了有不同内容标识符的程序或者使用了不同的记录和再现设备，也可以再现和使用在步骤 S702 中程序本地化选定为“否”的并在步骤 S707 中用根据系统共用密钥生成的保存数据加密密钥 Ksav 来加以加密的保存数据。

图 72 示出了一流程，它示出了用于再现通过图 20 的保存数据存储过程所存储的保存数据的过程。

在步骤 S711 中，记录和再现设备 300 读出内容 ID 例如游戏 ID。这是与图 70 所述的读出包含在内容数据的标识信息中的数据的步骤 S701 相类似的过程，

这种 ID 是先前图 4、26、27 和 32 至 35 所示的。在通过图 2 所示的接口接收到用于存储保存数据的命令时，主 CPU106 命令控制部 301 读取内容 ID。

在步骤 S712 中，从图 69 所示的记录设备 400 至 C 之一中读出参照图 71 所示的数据管理文件，并从中抽取出在步骤 S711 读出的内容 ID 和相应设置的程序本地化。如果数据管理文件具有置成“是”的程序本地化，则处理过程前进至步骤 S714，而如果数据管理文件具有置成“否”的程序本地化，则处理过程前进至步骤 S717。

在步骤 S714 中，从内容数据中读出内容独有的密钥例如内容密钥 Kcon 并将其用作保存数据解密密钥 Ksav，或者根据内容独有的密钥生成保存数据解密密钥 Ksav。这种解密密钥生成过程使用与加密密钥生成过程相对应的处理算法，即使用了这样的解密密钥生成算法，该算法能用根据某一内容独有密钥生成的解密密钥对根据同一内容独有密钥加密的数据进行解密。

另一方面，如果在步骤 S712 中判断出数据管理文件具有置成“否”的程序本地化，则在步骤 S717 中从记录和再现设备 300 的内部存储器 307 中读出存储在记录和再现设备 300 中的系统共用密钥并将其用作保存数据解密密钥 Ksav，或者，根据系统签名密钥 Ksys 生成保存数据解密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据密码翻译密钥 Ksav。

在步骤 S715 中，用在步骤 S714 或 S717 中选定或生成的保存数据解密密钥 Ksav 执行对保存数据进行解密的过程，在步骤 S716 中，在记录和再现设备 300 中再现和执行解密的保存数据。

因此，完成了用于保存数据再现过程。如果数据管理文件具有置成“是”的程序本地化，则根据内容独有密钥生成保存数据解密密钥，而如果数据管理文件具有置成“否”的程序本地化，则根据系统共用密钥生成保存数据解密密钥。如果数据管理文件具有置成“是”的程序本地化，则在没有用于内容的同样内容 ID 的情况下解密密钥不能对保存数据进行解密。

图 73 和 74 分别示出了保存数据存储和再现流程，该流程用内容 ID 生成保存数据加密和解密密钥。

在图 73 中，步骤 S721 至 722 与图 70 中的步骤 S701 和 702 相类似，故略去了对它们的说明。

图 73 中的保存数据存储流程，如果在步骤 S722 中程序本地化置成“是”，则在步骤 S723 中，从内容数据中读出内容 ID 并将其用作保存数据解密密钥 Ksav，或者，根据内容 ID 生成保存数据解密密钥 Ksav。例如，记录和再现设备 300 的密码翻译处理部 307 可将存储在记录和再现设备 300 的内部存储器中的主密钥 MKx 应用于从内容数据中读出的内容 ID，以便例如根据 DES(MKx，内容 ID)获得保存数据解密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据密码翻译密钥 Ksav。

另一方面，如果在步骤 S722 中将程序本地化置成“否”，则在步骤 S727 中，从内容数据中读出存储在记录和再现设备 300 中的系统共用密钥例如系统签名密钥 Ksys 并将其用作保存数据加密密钥 Ksav，或者，根据系统签名密钥生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

步骤 S724 及后续步骤的过程与图 70 的流程的步骤 S704 和后续步骤的过程相类似，故略去了对它们的说明。

图 74 示出了用于再现和执行于图 73 所示的保存数据存储流程过程中存储在记录设备内的保存数据的流程，除步骤 S734 以外，步骤

S731 至 S733 与图 72 所述的相应过程相类似。在步骤 S734 中，从内容数据中读出内容 ID 并将其用作保存数据解密密钥 Ksav，或者，根据内容 ID 生成保存数据解密密钥 Ksav。这种解密密钥生成过程使用与加密密钥生成过程相对应的处理算法，即使用了这样的解密密钥生成算法，该算法能用根据某一内容 ID 生成的解密密钥对根据同一内容 ID 加密的数据进行解密。

后续过程步骤 S735、S736 和 S737 类似于图 72 中的相应过程，故略去了对它们的说明。依照图 73 和 74 的保存数据存储和再现过程，如果程序本地化置成“是”，则内容 ID 用于生成保存数据加密和解密密钥，因此，如在用内容独有密钥的上述保存数据存储和再现过程中，在相应内容程序不匹配的情况下，不能获得保存数据，从而能将保存数据更安全地保存起来。

图 75 和 77 分别示出了保存数据存储(图 75)和再现(图 77)流程，该流程用记录和再现设备独有密钥生成保存数据加密和解密密钥。

在图 75 中，步骤 S741 与图 70 中的步骤 S701 相类似，故略去了对它的说明。在步骤 S742 中，为记录和再现设备设置或未设置本地化。在对能使用保存数据的特定记录和再现设备进行了本地化的情况下，即在记录和再现设备本地化也就是说使保存数据仅由已生成和存储数据的记录和再现设备所使用的情况下，将记录和再现设备本地化置成“是”，并且，为了使得其它记录和再现设备能使用保存数据，将记录和再现设备本地化置成“否”。如果在步骤 S742 中将记录和再现设备本地化置成“是”，则处理过程前进至步骤 S743，如果将本地化置或“否，”则处理过程前进至步骤 S747。

图 76 示出了数据管理文件的一个实例。数据管理文件被生成为一个表，它包含有条目，条目包括数据号、内容 ID、记录和再现设备 ID 和记录和再现设备本地化。内容 ID 是用于为其保存了保存数据的内容程序。记录和再现设备 ID 表示已存储了保存数据的记录和再现设备，它的一个实例是图 69 所示的[IDdev]。记录和再现设备本地化设置成“是”，以便将保存数据的使用限于特定的记录和再现设备，即使得保存数据仅由已生成和存储了数据的记录和再现设备所使用，或者，记录和再现设备本地化设置成“否”，以便使其它记录和再现设备使用保存数据。记录和再现设备本地化可由用户用内容程序来任意地设

置或者可以由内容产生者来设置并存储到内容程序中。

在图 75 的保存数据存储流程中。如果在步骤 S742 中将记录和再现设备本地化置成“是”，则从记录和再现设备 300 的内部存储器 307 中读出记录和再现设备独有的密钥例如记录和再现设备签名密钥 Kdev 并将其用作保存数据加密密钥 Ksav，或者，根据记录和再现设备签名密钥生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

另一方面，如果在步骤 S742 中判断出记录和再现设备本地化置成“否”，则在步骤 S747 中从记录和再现设备 300 的内部存储器 307 中读出存储在记录和再现设备 300 中的系统共用密钥例如系统签名密钥 Ksys 并将其用作保存数据加密密钥 Ksav，或者，根据系统签名密钥生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

步骤 S744 至 725 中的处理与上述图 72 的流程中的相应处理相类似，故略去了对它们的说明。

在步骤 S746 中，将内容 ID、记录和再现设备 ID 和用户在步骤 S742 中设置的记录和再现设备本地化“是/否”写至数据管理文件(见图 76)。

此外，图 77 示出了用于再现和执行于图 73 所示的保存数据存储流程过程中存储在记录设备内的保存数据的流程。在步骤 S751 中，如在上述图 72 的相应过程中那样，读出内容 ID。然后，在步骤 S752 中，读出存储在记录和再现设备 300 的存储器中的记录和再现设备 ID(IDdev)。

在步骤 S753 中，从数据管理文件中读出内容 ID、记录和再现设备 ID 和用户在步骤 S742 中设置的记录和再现设备本地化“是/否”(见图 76)。如果数据管理文件中具有相同内容 ID 的任何条目使记录和再现设备本地化置成“是”，如果表条目具有不同于在步骤 S752 中读出的记录和再现设备 ID，则处理过程结束。

如果在步骤 S754 中判断出数据管理文件使记录和再现设备本地化置成“是”，则处理过程前进至步骤 S755。如果数据管理文件使记录

和再现设备本地化置成“否”， 则处理过程前进至步骤 S758。

在步骤 S755 中，从记录和再现设备 300 的内部存储器 307 中读出记录和再现设备签名密钥 Kdev 并将其用作保存数据解密密钥 Ksav，或者，根据记录和再现设备签名密钥 Kdev 生成保存数据加密密钥 Ksav。这种解密密钥生成过程使用与加密密钥生成过程相对应的处理算法，即使用了这样的解密密钥生成算法，该算法能用根据某一记录和再现设备独有密钥生成的解密密钥对根据同一记录和再现设备独有密钥加密的数据进行解密。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

另一方面，在步骤 S758 中从记录和再现设备 300 的内部存储器 307 中读出存储在记录和再现设备 300 中的系统共用密钥例如系统签名密钥 Ksys 并将其用作保存数据解密密钥 Ksav，或者，根据系统签名密钥生成保存数据解密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。后续步骤 S756 至 757 中的处理与上述保存数据再现流程中的相应步骤内的处理相类似，故略去了对它们的说明。

依照图 75 和 77 所示的保存数据存储和再现过程，用记录和再现设备独有密钥对为其将记录和再现设备本地化置成“是”的保存数据加密。这些保存数据可加以解密并仅由具有同样记录和再现设备独有密钥的记录和再现设备即同一记录和再现设备所使用。

图 78 和 79 示出了用于用记录和再现设备 ID 生成保存数据的加密和解密密钥以及存储和再现保存数据的流程。

在图 78 中，记录和再现设备 ID 用于对记录设备中的保存数据进行加密并将其存储起来。在步骤 S764 中，从记录和再现设备中读出的记录和再现设备 ID(IDdev)用于生成保存数据加密密钥 Ksav。根据 IDdev 通过例如将 IDdev 用作保存数据加密密钥 Ksav 或用存储在记录和再现设备 300 的内部存储中的主密钥 MKx 而获得保存数据加密密钥 Ksav，从而根据 DES(MKx， IDdev)获得保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

后续步骤 S765 至 S768 与图 75 的相应处理流程相类似，故略去了对它们的说明。

图 79 示出了用于通过图 78 的处理过程再现和执行存储在记录设备中的保存数据的过程。步骤 S771 至 774 与图 77 中的相应处理过程相类似，故略去了对它们的说明。

在步骤 S775 中，从记录和再现设备中读出的记录和再现设备 ID(IDdev)用于生成保存数据解密密钥 Ksav。根据 IDdev 通过例如将 IDdev 用作密钥 Ksav 或用存储在记录和再现设备 300 的内部存储中的主密钥 MKx 而获得保存数据加密密钥 Ksav,从而根据 DES(MKx, IDdev)获得密钥 Ksav。这种解密密钥生成过程使用与加密密钥生成过程相对应的处理算法，即使用了这样的解密密钥生成算法，该算法能用根据某一记录和再现设备独有密钥生成的解密密钥对根据同一记录和再现设备独有密钥加密的数据进行解密。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

后续过程步骤 S776 至 S778 类似于图 76 中的相应过程。

依照图 78 和 79 所示的的保存数据存储和再现流程，用记录和再现设备独有密钥对为其将记录和再现设备本地化置为“是”的保存数据进行加密和解密。这些保存数据可加以解密并仅由具有同样记录和再现设备独有密钥的记录和再现设备即同一记录和再现设备所使用。

以下参照图 80 至 82 说明执行上述程序本地化及记录和再现设备本地化的保存数据存储和再现过程。

图 80 示出了保存数据存储流程。在步骤 S781 中，从内容数据中读出内容 ID，在步骤 S782 中，判断是否设置了程序本地化，在步骤 S783 中，判断是否设置了记录和再现设备本地化。

如果程序本地化和记录和再现设备本地化均置成“是”，则在步骤 S785 中,根据内容独有密钥(例如 Kcon)及记录和再现设备独有密钥(Kdev) 生成保存数据加密密钥 Ksav。例如根据 Ksav=(Kcon XOR Kdev)或者通过用存储在记录和再现设备 300 的存储器中的主密钥 MKx 而生保存数据加密密钥，以便根据 Ksav=DES(MKx, Kcon XOR Kdev)获得上述密钥。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥

Ksav。

如果程序本地化置成“是” 而记录和再现设备本地化置成“否”，则在步骤 S786，将内容独有密钥(例如 Kcon)用作保存数据加密密钥 Ksav，或者，根据内容独有密钥(例如 Kcon)生成保存数据加密密钥 Ksav。

如果程序本地化置成“否” 而记录和再现设备本地化置成“是”，则在步骤 S787，将记录和再现设备独有密钥(Kdev)用作保存数据加密密钥 Ksav，或者，根据记录和再现设备独有密钥(Kdev)生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

如果程序本地化和记录和再现设备本地化均置成“否”，则在步骤 S787 中，将系统共用密钥例如系统签名密钥 Ksys 用作保存数据加密密钥 Ksav，或者，根据系统签名密钥 Ksys 生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

在步骤 S789 中，在步骤 S785 至 S788 之一中生成的保存数据加密密钥 Ksav 用于对保存数据进行解密，然后将其存储到记录设备内。

此外，在步骤 S790 中，将在步骤 S782 和 S783 中设置的本地化存储在数据管理文件中。数据管理文件例如如图 81 所示那样配置并包含有条目，这些条目包括数据号、内容 ID、记录和再现设备 ID、程序本地化以及记录和再现设备本地化。

图 82A 和 82B 示出了用于通过图 80 的处理过程再现和执行存储在记录设备中的保存数据的过程。在步骤 S791 中，从执行程序中读出内容 ID 和记录和再现设备 ID，在步骤 S792 中，从数据管理文件中读出内容 ID、记录和再现设备 ID、程序本地化和记录和再现设备本地化。在这种情况下，如果程序本地化置成“是”且内容 ID 是不同的，或者，如果记录和再现设备本地化置成“是”且记录和再现设备 ID 是不同的，则处理过程结束。

然后，在步骤 S793、S794 和 S795 中，根据记录在数据管理文件中的数据，将解密密钥生成过程设置成步骤 796 至 S799 中的四种方式

之一。

如果程序本地化和记录和再现设备本地化均置成“是”，则在步骤 S796 中，根据内容独有密钥(例如 Kcon)及记录和再现设备独有密钥(Kdev) 生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。如果程序本地化置成“是” 而记录和再现设备本地化置成“否”，则在步骤 S797 中，将内容独有密钥(例如 Kcon)用作保存数据加密密钥 Ksav，或者，根据内容独有密钥(例如 Kcon)生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

如果程序本地化置成“否” 而记录和再现设备本地化置成“是”，则在步骤 S798 中，将记录和再现设备独有密钥(Kdev)用作保存数据加密密钥 Ksav，或者，根据记录和再现设备独有密钥(Kdev)生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。如果程序本地化和记录和再现设备本地化均置成“否”，则在步骤 S799 中，将系统共用密钥例如系统签名密钥 Ksys 用作保存数据加密密钥 Ksav，或者，根据系统签名密钥 Ksys 生成保存数据加密密钥 Ksav。另外，可将与业已被独立保存至记录和再现设备 300 的内部存储器 307 中的其它密钥不同的密码翻译密钥用作保存数据解密密钥 Ksav。

这些解密密钥生成过程使用与加密密钥生成过程相对应的处理算法，即使用了这样的解密密钥生成算法，该算法能用根据相同的内容独有密钥及记录和再现设备独有密钥生成的解密密钥对根据相同的内容独有密钥及记录和再现设备独有密钥加密的数据进行解密。

在步骤 S800 中，用在步骤 S796 至 S799 之一中生成的保存数据加密密钥 Ksav 执行解密过程，并在记录和再现设备中再现和执行解密的保存数据。

依照图 80 和 82 所示的的保存数据存储和再现流程，用内容独有密钥对为其将程序本地化置为“是”的保存数据进行加密和解密，因此，这些保存数据可加以解密并仅在使用具有同样内容独有密钥的的

情况下使用。另外，用记录和再现设备 ID 对为其将记录和再现设备本地化置为“是”的保存数据进行加密和解密，因此，这些保存数据可加以解密并仅由有同样记录和再现设备 ID 的记录和再现设备即同样的记录和再现设备所使用。所以，内容以及记录和再现设备可设置本地化，以便提高保存数据的保密性。

尽管图 80 和 82 示出了用于用内容独有密钥及记录和再现设备独有密钥来生成保存数据加密密钥以及解密密钥的结构，但是，也可用内容 ID 及记录和再现设备 ID 来分别代替内容独有密钥及记录和再现设备独有密钥，以根据这些 ID 生成保存数据加密密钥和解密密钥。

以下参照图 83 至 85 说明根据用户输入的口令来生成加密和解密密钥的结构。

图 83 示出了用于根据用户输入的口令来生成加密和解密密钥并将保存数据存储进记录设备内的流程。

在步骤 S821 中，如在上述各过程中那样从内容数据读出内容 ID。在步骤 S822 中，用户判断是否设置了程序本地化。在这种结构中设置的数据管理文件具有例如图 84 所示的结构。

如图 84 所示，数据包括数据号、内容 ID、记录和再现设备 ID 以及用户设置的程序本地化。“用户设置的程序本地化”是这样的条目，它判断程序的使用是否限于特定的用户。

如果在图 83 的流程的步骤 S822 中本地化置成“是”，则在步骤 S823 中输入用户口令。该口令是从诸如图 2 所示键盘之类的输入装置中输入的。

在主 CPU106 和控制部 301 的控制下将输入的口令输出给密码翻译处理部 302，并且，执行步骤 S824 中的处理过程，也就是说，根据输入的用户口令生成保存数据加密密钥 Ksav。可通过例如将口令本身设置成密钥 ksav 或者使用记录和再现设备的主密钥 MKx 而生成保存数据加密密钥 Ksav，以便根据保存数据加密密钥 Ksav=DE(MKx，口令)来生成密钥 Ksav。另外，可通过将口令用作输入而应用单向函数，从而可根据来自该函数的输出生成加密密钥。

如果用户本地化在步骤 S822 中置成“否”，则在步骤 S828 中，根据记录和再现设备 300 的系统共用密钥生成保存数据加密密钥。

在步骤 S825 中，用在步骤 S824 至 S828 生成的保存数据加密密钥

Ksav对保存数据进行加密，在步骤S826中，将加密的保存数据存储到记录设备内。

在步骤S827中，将用户在步骤S822中程序本地化将写至图84中的数据管理文件，以便与内容ID、记录和再现设备ID关联起来。

图85示出了用于再现通过图83的处理过程存储起来的保存数据的过程。在步骤S831中，从内容数据中读出内容ID，在步骤S832中，从图84的数据管理文件中读出内容ID、记录和再现设备ID和用户设置的程序本地化。

在步骤S833中，根据数据管理文件中的数据进行判断。如果“用户设置的程序本地化”置成了“是”，则在步骤S834中提示用户输入口令，在步骤S835中，根据输入的口令生成解密密钥。这种解密密钥生成过程使用与加密密钥生成过程相对应的处理算法，即使用了这样的解密密钥生成算法，该算法能用根据相同的口令生成的解密密钥对根据相同的口令加密的数据进行解密。

如果在步骤S833中判断出用户设置的程序本地化置成“否”，则在步骤S837中，存储在记录和再现设备300的内部存储器中的系统共用密钥用于通过用系统签名密钥Ksys生成保存数据解密密钥Ksav。另外，可将与业已被独立保存至记录和再现设备300的内部存储器307中的其它密钥不同的加密密钥用作保存数据加密密钥Ksav。

在步骤S836中，在步骤S835或S839中生成的解密密钥Ksav用于对存储在记录设备中的保存数据进行解密，在步骤S836中，记录和再现设备再现并执行保存数据。

依照图83和85所示的的保存数据存储和再现流程，根据用户输入的口令用密钥对为其将“用户设置的程序本地化”选择为“是”的保存数据进行加密和解密，因此，这些保存数据可加以解密并仅在输入了同样的口令的情况下使用，从而提高保存数据的保密性。

业已说明了保存数据存储和再现过程的若干方面，但是，也可以实现通过将上述过程例如使用口令、记录和再现设备ID、内容ID等生成保存数据加密和解密密钥的方面结合起来所获得的过程。

(17)用于排除(撤消)非法设备的结构

如前所述，本发明的数据处理设备利用这样的结构提高了所提供内容的保密性并使得这种内容仅为有效用户使用，在所述结构中，记

录和再现设备 300 对介质 500(见图 3)或通信装置 600 提供的多种内容数据执行诸如鉴别和加密之类的处理，然后将所述数据存储进记录设备内。

从上述说明中看出，用存储在记录和再现设备 300 的密码翻译处理部 302 的内部存储器 307 中的多种签名密钥、主密钥和整体性检查值生成密钥（见图 8）对输入内容进行鉴别、加密和解密。存储有密钥信息的内部存储器 307 的最佳特征是防止外部非法读取，因为，该存储器包括半导体芯片，该芯片能基本上拒绝外部访问并具有多层结构、在铝或类似材料制成的哑层之间的或设置在最低层上的内部存储器以及狭窄范围的工作电压和/或频率。但是，如果要从内部存储器中读出密钥数据或类似数据并将具拷贝给未鉴别的记录和再现设备，则拷贝的密钥信息可用于无效地使用内容。

以下说明防止以密钥的无效拷贝为基础的无效使用内容的结构。

图 86 是用于说明“(17) 用于排除(撤消)非法设备的结构”的框图。记录和再现设备 300 与上述图 2 和 3 中所示的记录和再现设备相类似，并且具有内部存储器和前述多种密钥数据(见图 18)以及记录和再现设备 ID。这里，由第三方拷贝的记录和再现设备 ID、密钥数据或类似数据不一定存储在内部存储器 307 内，而图 86 所示的记录和再现设备 300 中的密钥数据则以集合的方式或分布的方式存储在可为密码翻译处理部 302 所访问的存储部内(见图 2 和 3)。

为了实现用于排除无效设备的结构，无效记录和再现设备 ID 的列表存储在内容数据的头标部中。如图 86 所示，内容数据保存有一撤消列表，该列表用作无效记录和再现设备 ID(IDdev)的列表。再有，列表整体性检查值 ICVrev 用于撤消列表的篡改情况。无效记录和再现设备 ID(IDdev)的列表包含有内容提供者或管理者根据无效拷贝等的分布状态确定的无效记录和再现设备的标识符 IDvev。可用发布密钥 Kdis 在存储之前对撤消列表加密。记录和再现设备所执行的解密过程例如与图 22 中的内容下载过程的解密过程相类似。

这里，为了更好地加以理解，撤消列表被显示为图 86 的内容数据中的单个数据，但是，撤消列表可例如包含在前述使用策略(例如见图 32 至 35)内，使用策略是内容包含的头标部的组成部。在这种情况下，前述整体性检查值 ICVa 用于检查包含撤消列表的使用策略数据的篡改

情况。如果撤消列表包含在使用策略内，则整体性检查值 A: ICVa 用于上述检查，并且，使用记录和再现设备中的整体性检查值 A 生成密钥 Kicva，从而消除存储整体性检查值生成密钥 Kicv-rev 的需要。

如果作为独立数据撤消列表包含在内容数据中，则用列表整体性检查值 ICVrev 来检查撤消列表，以检查撤消列表的篡改情况，并且，根据列表整体性检查值 ICVrev 和内容数据中的其它部分整体性检查值生成中间整体性检查值，并将该中间整体性检查值用于执行验证过程。

用于用列表整体性检查值 ICVrev 检查撤消列表以检查撤消列表的篡改情况的方法类似于用来生成如图 23 和 24 所述的诸如 ICVa 或 ICVb 之类整体性检查值的过程。也就是说，依照图 23 和 24 及其它图所示的 ICV 计算方法在将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的整体性检查值生成密钥 Kicv-rev 用作密钥并将包含在数据数据中的撤消列表用作消息的情况下进行计算。计算出的整体性检查值 Kicv-rev'和存储在头标中的检查值整体性检查值 Kicv-rev 一起作比较，如果它们相等，则判定列表未被篡改。

例如通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的总体整体性检查值生成密钥 Kicvt 用作密钥并将图 7 及其它图所示的 ICV 计算方法应用于消息串，从而包含列表整体性检查值 ICVrev 的生成中间整体性检查值，所述消息串包括整体性检查值 A 和 B 以及验证的头标内的列表整体性检查值 ICVrev，根据图 25 所示的格式增加内容整体性检查值。

通过诸如 DVD 或 CD 之类的介质 500 或通信装置 600 或诸如存储卡之类的记录设备 400 将撤消列表和列表整体性检查值提供给记录和再现设备 300。在这种情况下，记录和再现设备 300 保存在有效密钥内容或非法拷贝的 ID。

图 87 和 88 示出了本结构中用于排除无效记录和再现设备的过程的流程。图 87 示出了在通过诸如 DVD 或 CD 之类的介质 500 或通信装置 600 提供内容的情况下用于排除（撤消）无效记录和再现设备的过程的流程，而图 88 示出了在通过诸如存储卡之类的记录设备 400 提供内容的情况下用于排除（撤消）无效记录和再现设备的过程的流程。

首先说明图 87 中的流程。在步骤 S901 中，安装介质并请求内容，

即请求再现或下载过程。图 87 所示的过程与例如在将诸如 DVD 等之类的介质安装到记录设备之前的步骤相对应，所进安装过程的后面是下载过程。下载过程如参照图 22 所述并且是作为在图 22 的流程之前的步骤或插进这一流程中中的一个过程而执行的。

如果记录和再现设备 300 通过诸如网络之类的通信装置接收到了内容，则在步骤 S911 中，形成与内容发布服务方的通信会话，然后处理过程前进至步骤 S902。

在步骤 S902 中，从内容数据的头标部获得撤消列表(见图 86)。在这一列表获得过程中，如果介质中存在有内容，则图 3 所示的控制部 301 就通过读取部 304 从介质中读出内容。如果内容是从控制部中获得的，则图 3 所示的通信装置 301 就通过通信部 305 从内容发布、万接收内容。

在步骤 S903 中，控制部 301 将从介质 500 或通信装置 600 中获得的撤消列表传给密码翻译处理部 302，然后便密码翻译处理部 302 执行检查值生成过程。记录和再现设备 300 在内部具有撤消整体性检查值生成密钥 Kicv-rev、依照图 23 和 24 所述的 ICV 计算方法通过应用整体性检查值生成密钥 Kicv-rev 在将接收到的撤消列表用作消息的情况下计算整体性检查值 Kicv-rev'，并将计算结果与存储在头标中的整体性检查值 ICV-rev 作比较，以便在它们相等的情况下(步骤 S904 中的是)判断出列表未被篡改。如果值不相等，则记录和再现设备会判断出列表已被篡改，处理过程前进至步骤 S909，以表示过程出错，从而结束处理过程。

在步骤 S905 中，记录和再现设备密码翻译处理部 302 的控制部 306 使使记录和再现设备密码翻译处理部 302 的加密/解密部 308 计算总体整体性检查值 ICVt'。如图 25 所示，通过将存储在记录和再现设备密码翻译处理部 302 的内部存储 307 中的系统签名密钥 Ksys 用作密钥而生成总体整体性检查值 ICVt，以便根据 DES 对中间整体性检查值进行加密。图 87 所示的流程中略去了与诸如 ICVa 或 ICVb 之类的各部分整体性检查值的验证过程，但可根据数据格式如在图 39 至 45 作示的流程中那样执行与这些部分检查值的验证过程。

然后，在步骤 S906 中，所生成的总体整体性检查值 ICVt'和头标中的整体性检查值 ICVt 作比较，如果它们相等(步骤 S906 中的是)，

则处理过程前进至步骤 S907。如果这些值不相等，则记录和再现设备可断判出列表已被篡改，处理过程前进至步骤 S909，以表示过程出错，从而结束处理过程。

如前所述，总体整体性检查值 ICVt 用于检查包含在内容数据中诸如 ICVa 和 ICVb 之类的所有的部分整体性检查值以及用于取决于数据格式的相应内容块的整体性检查值。但是，在这种情况下，将用于检查撤消列表篡改情况的列表整体性检查值 ICVrev 增加给部分整体性检查值，并且，检查所有这些的整体性检查值的篡改情况。如果总体整体性检查值等于存储在头标中的整体性检查值 ICVt，则可判断出 ICVa 和 ICVb、内容块整体性检查值和列表整体性检查值 ICVrev 均未被篡改。

在步骤 S907 中，已判断出来被篡改的撤消列表与存储在记录和再现设备 300 内的记录和再现设备 ID(IDdev)作比较。

如果从内容数据中读出的无效记录和再现设备 ID IDdev 的列表包含该记录和再现设备的标识符 IDdev，则可判定该记录和再现设备 300 具有非法拷贝的密钥数据。然后，所述处理过程前进至步骤 S909，以便中断后续的过程。例如，所述过程例如图 22 中的内容下载过程的执行无效。

在步骤 S907 中，如果判断出无效记录和再现设备 ID IDdev 的列表不包含该记录和再现设备的标识符 IDdev，则可判定该记录和再现设备 300 具有有效的密钥数据。所述处理过程前进至步骤 S908，以便使后续的过程例如程序执行过程或图 22 或其它图中的内容下载过程有效。

图 88 示出了再现存储在诸如存储卡之类的记录设备 400 中的内容数据。如前所述，诸如存储卡之类的记录设备 40 与记录和再现设备 300 执行图 20 所示的相互鉴别过程(步骤 S921)。如果在步骤 S922 中相互鉴别成功，则所述处理过程前进至步骤 S923 和后续处理过程，而如果相互鉴别失败，则在步骤 S930 中出错，以便阻止执行后续处理过程。

在步骤 S923 中，从内容数据的头标部中获得撤消列表(见图 86)。后续步骤 S924 至 S930 中的处理过程与图 87 中的相应处理过程相类似。也就是说，用列表整体性检查值(S924 和 S9257 并用总体整体性检查值(S926 和 S927)来验证上述列表，并且，列表条目与记录和再现设

备 ID IDdev 相比较(S928)。如果无效记录和再现设备 ID IDdev 的列表包含该记录和再现设备的标识符 IDdev，则可判定该记录和再现设备 300 具有非法拷贝的密钥数据。然后，所述处理过程前进至步骤 S930，以便中断后续的过程。例如，所述过程例如图 22 中的内容下载过程的执行无效。另一方面，如果判断出无效记录和再现设备 ID IDdev 的列表不包含该记录和再现设备的标识符 IDdev，则可判定该记录和再现设备 300 具有有效的密钥数据，所述处理过程前进至步骤 S929，以便使后续的过程有效。

如前所述，依照本发明的内容处理设备，标识无效记录和再现设备的数据即包含无效记录和再现设备的标识符 IDdev 的撤消列表作为内容数据的头标部的组成数据包含在内容提供者或管理所提供的内容中。在使用记录和再现设备中的内容之前，记录和再现设备的用户比较存储在记录和再现设备的存储器中的记录和再现设备 ID IDdev 与列表中的 ID 并在发现有匹配数据的情况下阻止后续处理过程。因此，可防止将拷贝密钥数据存储在其存储器中的无效记录和再现设备使用内容。

(18)、用于配置和生产保密芯片的方法

如前所述，记录和再现设备密码翻译处理部 302 的内部存储器 307 或记录设备 400 的内部存储器 405 保存有诸如密码翻译密钥之类的重要信息，从而需要构建成能拒绝外部无效读取。因此，记录和再现设备密码翻译处理部 302 和记录设备密码翻译处理部 401 配置成为一防篡改的存储器，其特征在于防止外部非法读取，因为，它包括例如半导体芯片，此芯片能基本上拒绝外部访问并具有多层结构、在铝或类似材料制成的哑层之间或设置在最低层上的内部存储器以及狭窄范围的工作电压和/或频率。

但是，从以上说明中可以看出，诸如记录和再现设备签名密钥 Kdev 之类的随记录和再现设备而变的数据必须写至记录和再现设备密码翻译处理部 302 的内部存储器 307。此外，在用于各芯片的个别信息例如标识信息(ID)和加密密钥信息已写至芯片的非易失性存储区例如按块擦除存储器或 FeRAM 之后，例如在发货之后，必须使重写数据或读数据难以进行。

使数据读取和重写难以进行的通常方法例如包括使数据写命令协

议保密或将芯片上在完成生产之后使用的用于接收来自通信信号线的数据写命令的信号线分离出来，因此，数据写命令无效，除非是信号直接传给基层上的芯片。

但是，就这种通常的方法而言，具有存储部件技术知识的人能在有工具和用于驱动电路的技术的情况下将信号输出给芯片的数据写区域，并且，即便是数据写命令协议是保密的，也总是存在能对协议进行分析的可能性。

发布用于存储密码翻译处理数据的能使保密数据被修改的部件会威胁整个的密码翻译处理系统。此外，为了防止读出数据，可避免实施数据读取命令。但是，即便执行了合法的数据写入，也不能判断是否是精确地写入了已写的数据，从而导致提供其中写有不适当的数据的芯片。

就这些通常的技术而言，本发明提供了一种这样的保密芯片结构，它能使得数据被精确地写至诸如按块擦除的存储器或 FeRAM 之类的非易失性存储器，同时防止从中读出数据，而且，本发明还提供了一种用于制造这种保密芯片的方法。

图 89 示出了例如可应用于上述记录和再现设备密码翻译处理部 302 或记录设备 400 的密码翻译处理部 401 的保密芯片。图 89(A)示出了在芯片制造过程中即在数据写过程中形式的保密芯片结构，图 89(B)示出了诸如记录和再现设备 300 或记录设备 400 之类的产品的结构的实例，该结构具有安装在上述产品中并使数据写入其中的保密芯片。

在制造过程中，保密芯片的处理部 8001 具有与之相连的模式指定信号线 8003 和多种命令信号线 8004，并根据例如芯片处于数据写入模式还是数据读出模式将数据写至或读自存储部 8002，存储部 8002 包括非易失性存储器。

另一方面，在图 89(B)的安装有保密芯片的产品中，保密芯片通过通用信号线与从外部连接的接口、外围设备以及其它部件相连，而模式信号线 8003 则不连接。用于模式信号线 8003 的具体处理过程包括将信号线 8003 接地、将这些信号线上的电压增加至 Vcc、切割这些信号线、用绝缘树脂封住这些信号线等。这种处理能防止在发货之后访问保密芯片中的模式信号线，从而防止在外部从芯片中读出数据或将数据写至芯片。

此外，这种结构的保密芯片 8000 能防止将数据写至存储部 8002，同时能防止从存储部中读出写入的数据，从而，即使第三方成功地访问了模式信号线 8003，也能防止无效的数据写入或读出。图 90 示出了将数据写至上述结构的保密芯片或将数据从保密芯片中读出的流程。

在步骤 S951 中，就数据写或读模式设置模式信号线 8003。

在步骤 S952 中，从芯片中读出鉴别信息。这种结构的保密芯片例如通过连续或掩模 ROM 结构存储有鉴别过程所需的诸如口令之类的信息以及用于密码翻译技术的鉴别过程的密钥信息。在步骤 S952 中，读出鉴别信息是以执行鉴别过程。例如，如果通常的数据写装置和数据读装置与通用信号线相连以执行鉴别过程，那么，鉴别过程就是成功的(步骤 S953 中的是)。但是，如果无效的数据写装置和数据读装置与通用信号线相连以执行鉴别过程，那么，鉴别过程就失败(步骤 S953 中的否)，从而，处理过程停止。例如，可依照先前图 13 所述的相互鉴别处理过程来执行鉴别过程。图 89(A)所示的处理部 8001 具有这样的结构，它能进行这样的鉴别过程。这一点可例如用与包括在先前图 29 所示的密码翻译处理部 401 的控制部 407 中的命令寄存器相类似的结构加以实现。例如，图 89(A)的芯片的处理部具有与包括在先前图 29 所示的记录设备 400 的密码翻译处理部 401 的控制部 407 中的命令寄存器相类似的结构并执行适当的处理过程，以便响应来自与多条命令信号线 8004 相连的设备的预定命令输入而使鉴别过程序列得以执行。

如果鉴别过程成功，则处理部 8001 接受数据写或读命令，以执行数据写(步骤 S955)或读(步骤 S956)处理。

如上所述，这种结构的保密芯片配置成能对数据写或读执行鉴别过程，从而防止不合法的第三方从保密芯片的存储部中读数据或将数据写入上述存储部内。

图 91 示出了保密部件结构的一个实施例。在该例中，保密芯片的存储部 8200 被分成两个区域：一个区域是读写(RW)区域 8201，可将数据写入其中并从中读出数据，另一个是只写(WO)区域 8202，只能将数据写入其中。

在这种结构中，将需要高度保密性的密码翻译密钥数据、ID 数据和其它数据写至只写(WO)区域 8202，而将不需要如此高度保密性的整体性检查值和其它数据写至读写(RW)区域 8201。

作为从读写(RW)区域 8201 中读出数据的过程，处理部 8001 执行数据读过程，该过程包括图 90 所述的鉴别过程。但是，在图 92 的流程之后执行数据写过程。

在图 92 的步骤 S961 中，就写模设置模式信号线 8003，在步骤 S962 中，执行与以上图 90 作述相类的鉴别过程。当鉴别过程成功时，处理过程前进至步骤 S963，以便将用于把诸如密钥数据之类需要高度保密性的信息写至只写(WO)区域 8202 中的命令通过命令信号线 8004 输出给处理部 8001，同时将不需要如此高度保密性的检查数据或其它数据写至读写(RW)区域 8201。

在步骤 S964 中，在接收到命令时，处理部 8001 根据该命令对只写(WO)区域 8202 或读写(RO)区域 8201 执行数据写过程。

此外，图 93 示出了用于对写至只写(WO)区域 8202 的数据进行验证的流程。

在图 93 的步骤 S971 中，处理部 8001 根据写入的数据使只写(WO)区域执行密码翻译处理过程。与上述鉴别过程执行结构相类似，本执行结构是用顺序执行存储在命令寄存器中的密码翻译处理过程序列的结构来实现的。此外，处理部 8001 中执行的密码翻译处理算法没有特别的限制，而是例如可以执行前述 DES 算法。

在步骤 S972 中，与保密芯片相连的验证设备从处理部 8001 接收密码翻译处理过程的结果。在步骤 S973 中，将与处理部 8001 对在步骤 S973 中被写至存储部的合法写数据执行的算法相类似的密码翻译处理过程应用结果和来自处理部 8001 的加密结果作比较。

如果比较的结果是相同的，则验证出写至只写(WO)区域 8202 的数据是正确的。

利用这种结构，如果鉴别过程应被解释成执行读命令，则可仅从读写(RW)区域 8201 中读出数据，同时，不能读出被写至只写(WO)区域 8202 的数据，从而，这种结构能提供很高的保密性。此外，与阻止数据读出的芯片不同，本芯片包括读写(RW)区域 8201，以便确实能访问存储器。

业已参照具体实施例说明了本发明。但是，很明显，在不偏离本发明精神的情况下本领域的技术人员可形成本发明的改进或替代形式。也就是说，仅就说明的目的公开了本发明，不应按限制的方式来

解释本发明。此外，在上述实施例中，以举例的方式说明了能记录和再现内容的记录和再现设备。但是，本发明的结构可应用于能仅记录或再现数据的设备，并且，可用个人计算机、游戏设备和其它多种数据处理设备在总体上实现本发明。为了确定本发明的要点，应参照本申请的权利要求书。

产业上的可利用性

本发明可用于能再现诸如声音、图像、游戏和程序之类的多种内容的设备和系统，上述内容是通过诸如 DVD 和 CD 之类存储介质或通过诸如 CATV、因特网和卫星通信之类的多种有线和无线通信获得的，在记录和再现过程中，用户将内容存储到诸如存储卡、硬盘和 CD-R 之类特定记录设备内，同时，上述设备和系统能提供保密性，其中，就使用存储在记录设备中的内容而言，对内容提供想要的利用进行限制，并且，可防止合法用户以外的第三方非法使用所提供的内容。

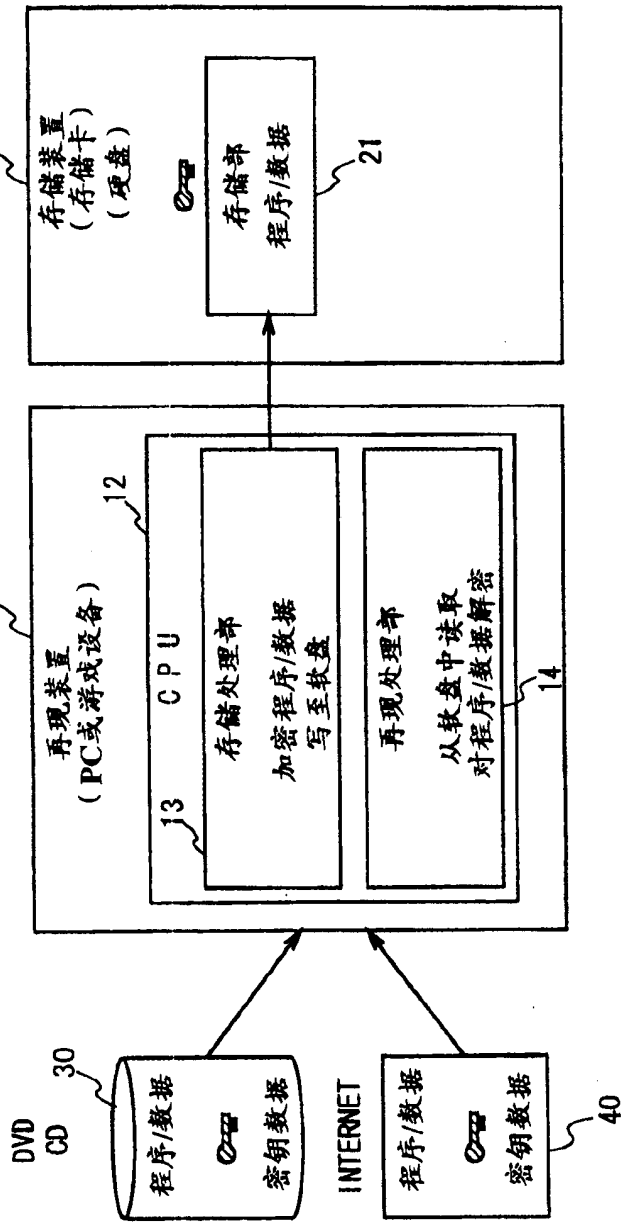

20
存储装置
(存储卡)
(硬盘)
21
存储部
程序/数据
10
再现装置
(PC或游戏设备)
12
CPU
13
存储处理部
加密程序/数据
写至软盘
再现处理部
从软盘中读取
对程序/数据解密
14
30
DVD
CD
程序/数据
密钥数据
INTERNET
程序/数据
密钥数据
40

图 1

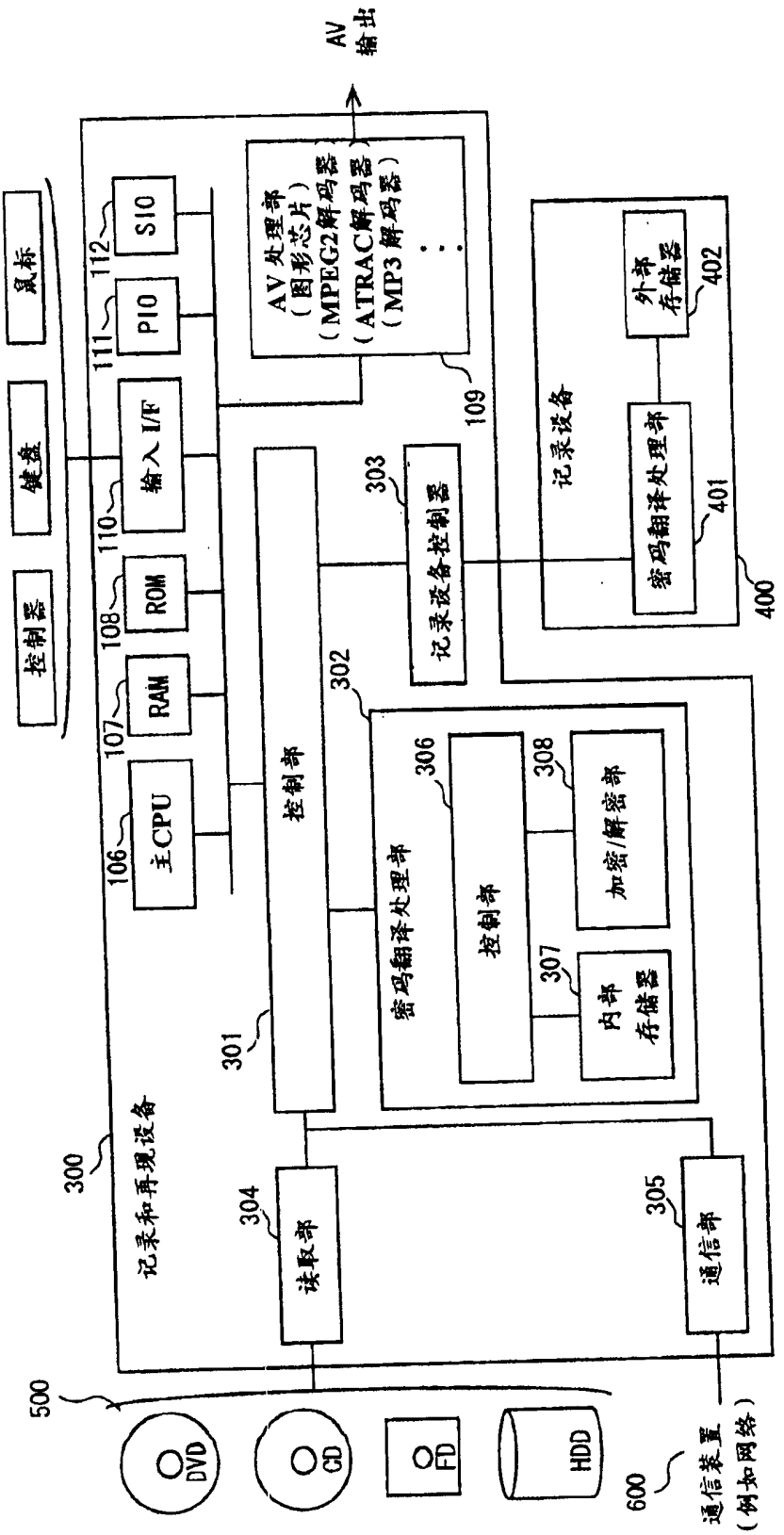

AV
输出
鼠标
键盘
控制器
S10
112
PIO
111
输入 I/F
110
ROM
108
RAM
107
主CPU
106
AV 处理部
（图形芯片）
（MPEG2解码器
（ATRAC解码器
（MP3 解码器）
109
记录设备
外部
存储器
402
密码翻译处理部
401
400
303
记录设备控制器
控制部
302
密码翻译处理部
306
控制部
308
加密/解密部
307
内部
存储器
301
记录和再现设备
300
304
读取部
305
通信部
500
DVD
CD
FD
HDD
600
通信装置
（例如网络）

图 2

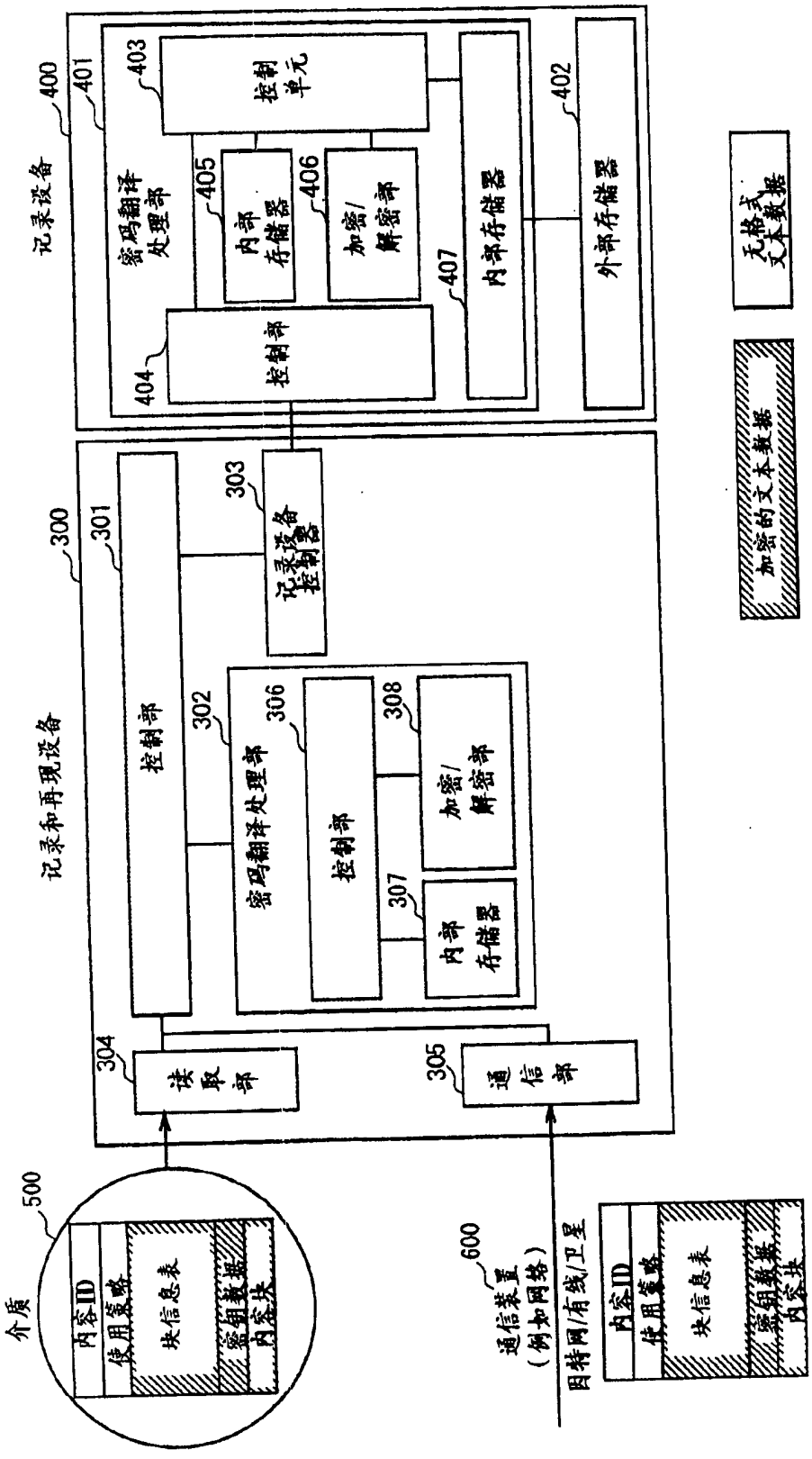
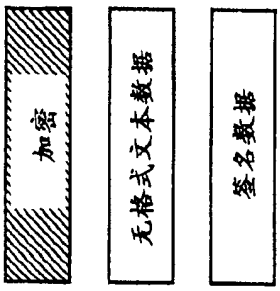
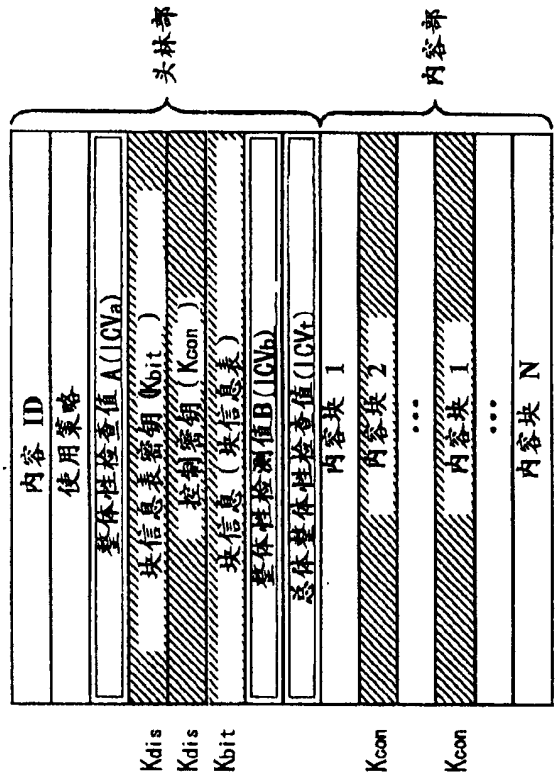

介质
500
内容ID
使用策略
块信息表
密钥数据
内容块
通信装置
(例如网络)
600
因特网/有线/卫星
记录和再现设备
300
读取部
304
通信部
305
控制部
301
密码翻译处理部
302
控制部
306
内部存储器
307
加密/解密部
308
记录设备控制器
303
记录设备
400
密码翻译处理部
401
控制单元
403
内部存储器
405
加密/解密部
406
控制部
404
内部存储器
407
外部存储器
402
加密的文本数据
无格式文本数据

图 3





介质和通信路径上的数据格式

图 4

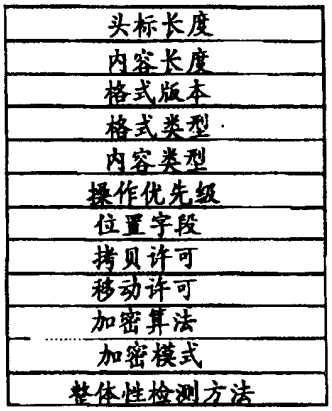
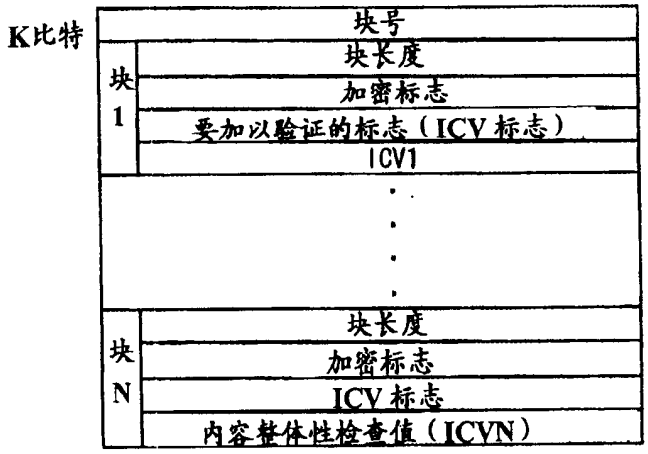

头标长度
内容长度
格式版本
格式类型
内容类型
操作优先级
位置字段
拷贝许可
移动许可
加密算法
加密模式
整体性检测方法
使用策略

图 5


K比特
块号
块1
块长度
加密标志
要加以验证的标志（ICV 标志）
ICV1
块N
块长度
加密标志
ICV 标志
内容整体性检查值（ICVN）

块信息表

图 6

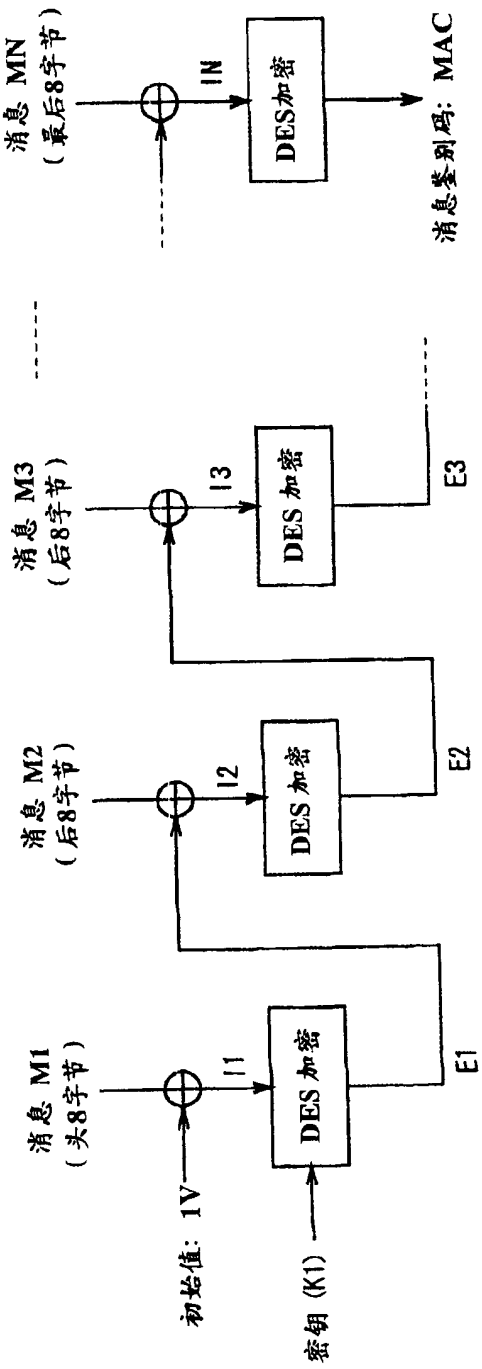


图 7

⊕：异或（XOR）处理过程（8字节单元）

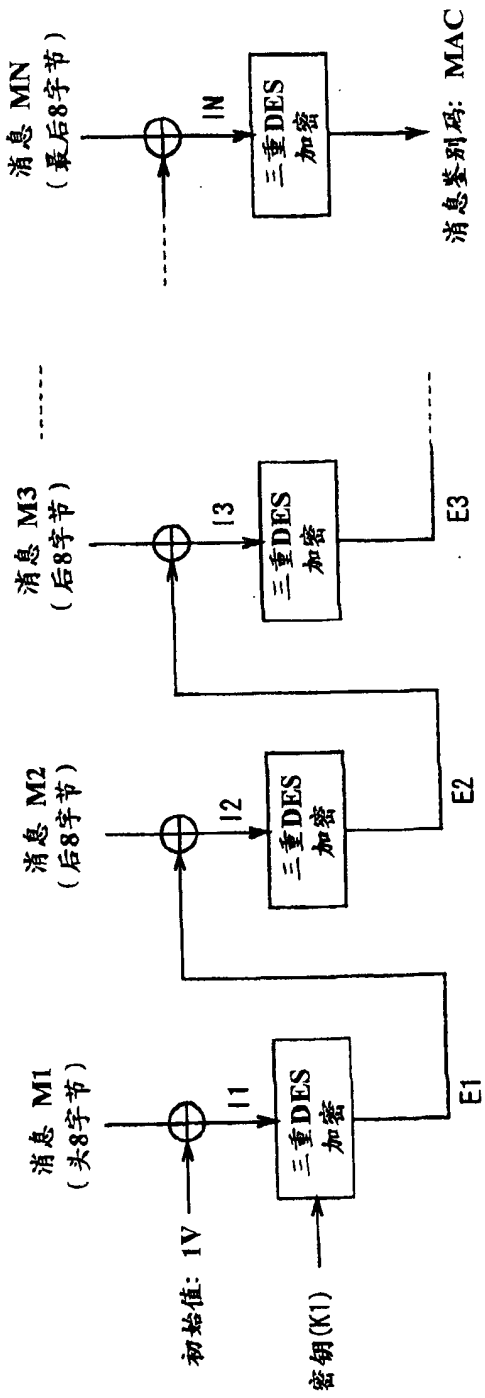

消息 M1
（头8字节）
初始值: IV
I1
三重DES
加密
密钥(K1)
E1
消息 M2
（后8字节）
I2
三重DES
加密
E2
消息 M3
（后8字节）
I3
三重DES
加密
E3
消息 MN
（最后8字节）
IN
三重DES
加密
消息鉴别码: MAC

图 8

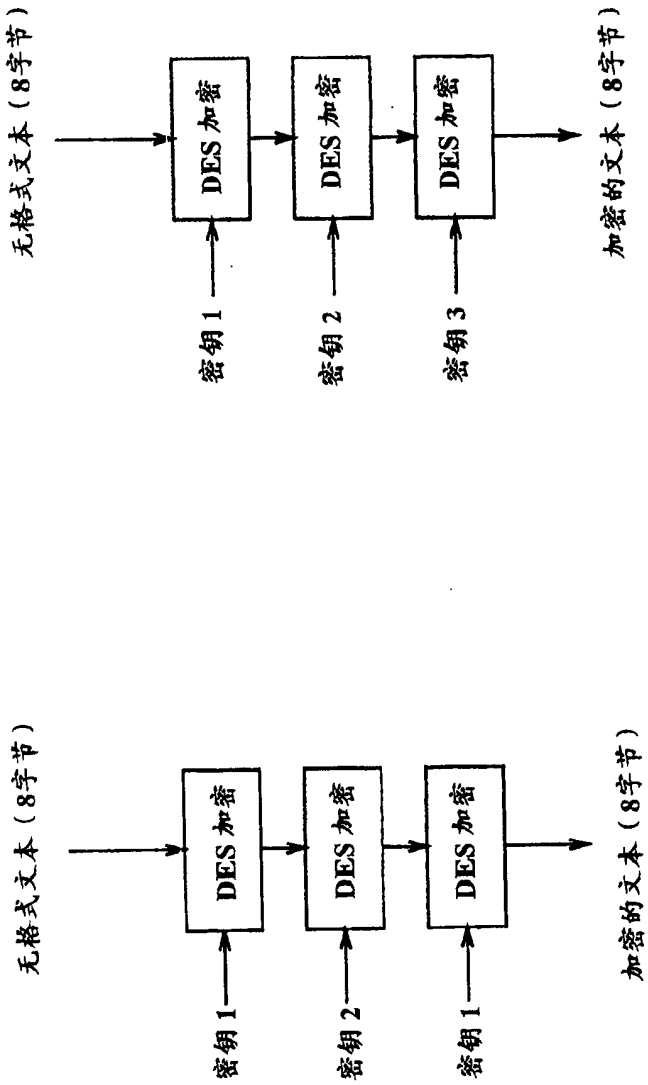

无格式文本（8字节）
DES 加密
DES 加密
DES 加密
密钥 1
密钥 2
密钥 3
加密的文本（8字节）
(B)
无格式文本（8字节）
DES 加密
DES 加密
DES 加密
密钥 1
密钥 2
密钥 1
加密的文本（8字节）
(A)

图 9

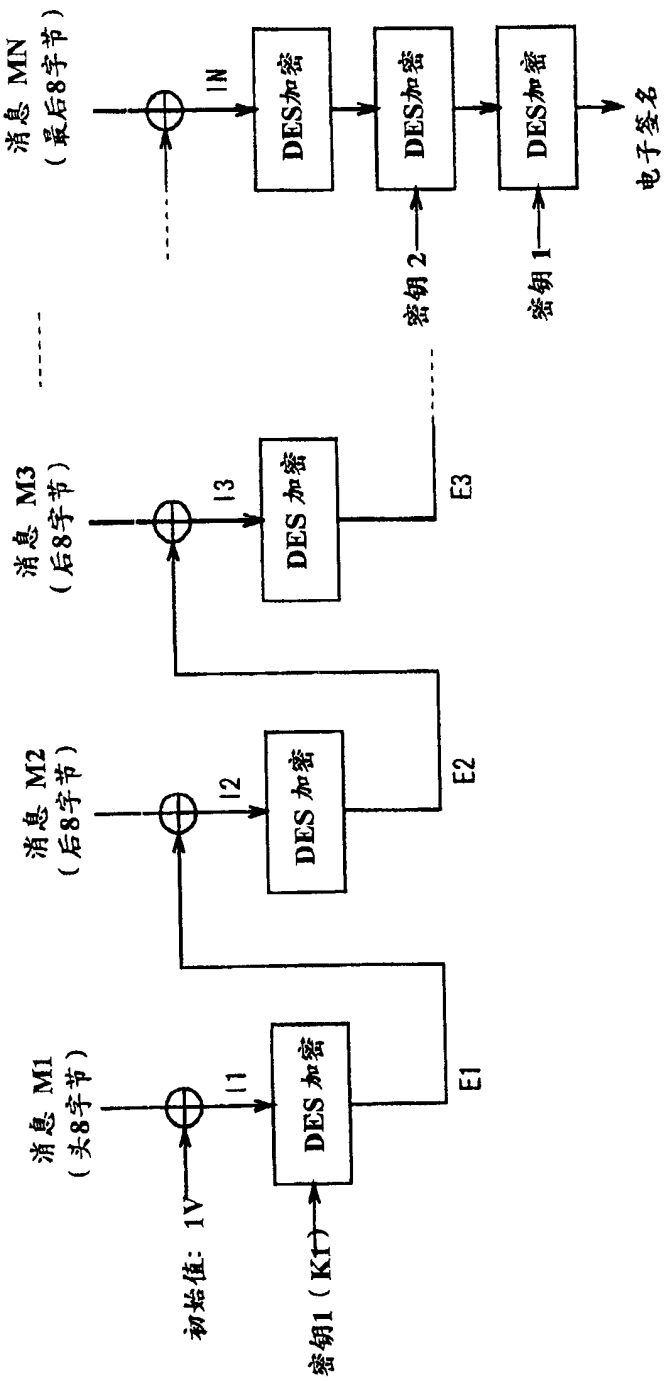

消息 M1
（头8字节）
消息 M2
（后8字节）
消息 M3
（后8字节）
消息 MN
（最后8字节）
初始值: 1V
密钥1（K1）
I1
I2
I3
IN
DES 加密
E1
E2
E3
DES加密
密钥 2
密钥 1
电子签名

图 10

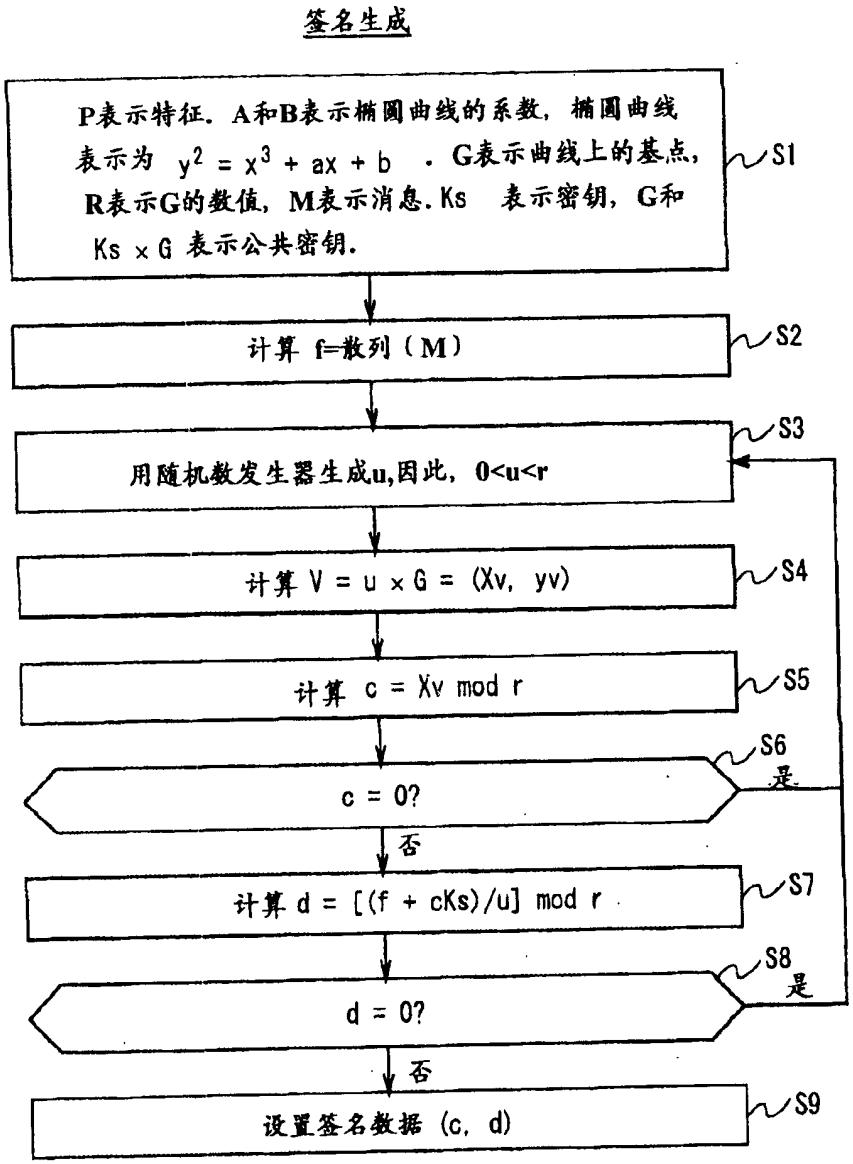
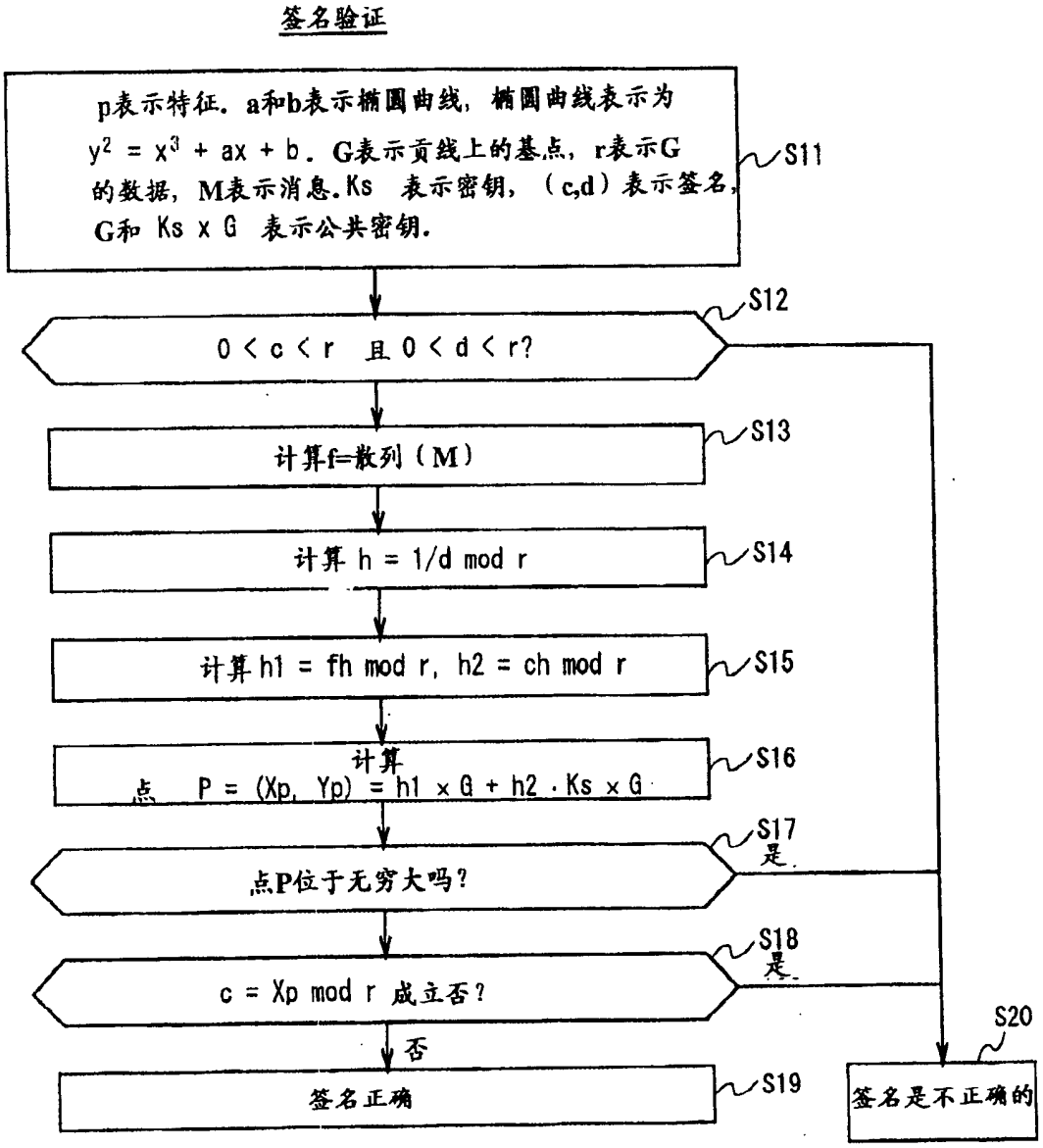
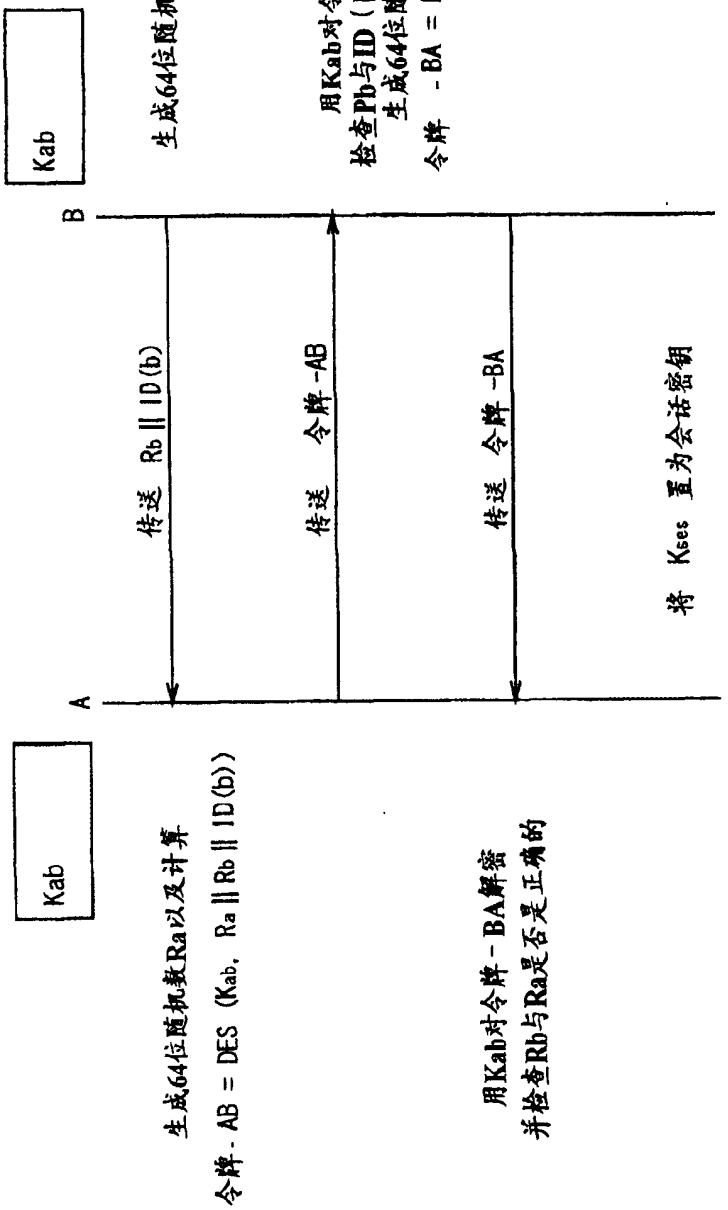

签名生成
P表示特征. A和B表示椭圆曲线的系数, 椭圆曲线表示为 $y^2 = x^3 + ax + b$. G表示曲线上的基点, R表示G的数值, M表示消息. Ks 表示密钥, G和 Ks × G 表示公共密钥.
S1
计算 f=散列（M）
S2
用随机数发生器生成u,因此, 0<u<r
S3
计算 V = u × G = (Xv, yv)
S4
计算 c = Xv mod r
S5
c = 0?
S6
是
否
计算 d = [(f + cKs)/u] mod r
S7
d = 0?
S8
是
否
设置签名数据 (c, d)
S9
生成签名 (IEEE P1363/D3)

图 11



签名验证(IEEE P1363/D3)

图 12



使用对称密钥密码翻译技术的ISO/IEC9798-2相互鉴别和密钥共享方法

图 13

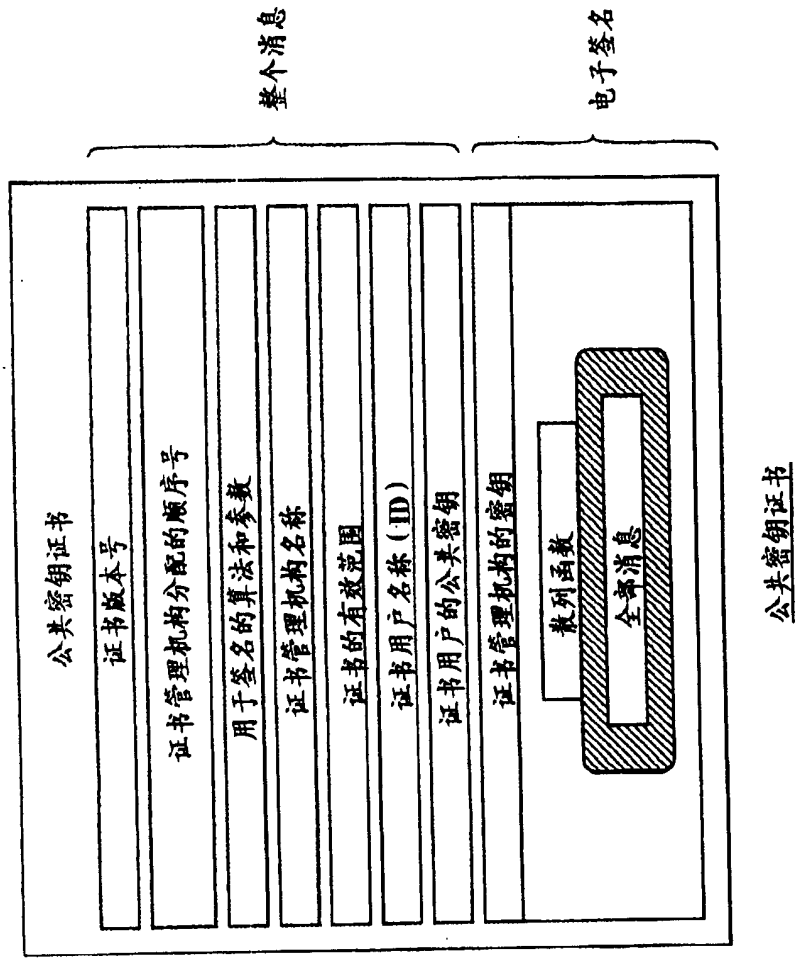

公共密钥证书
证书版本号
证书管理机构分配的顺序号
用于签名的算法和参数
证书管理机构名称
证书的有效范围
证书用户名称（ID）
证书用户的公共密钥
证书管理机构的密钥
散列函数
全部消息
整个消息
电子签名
公共密钥证书

图 14

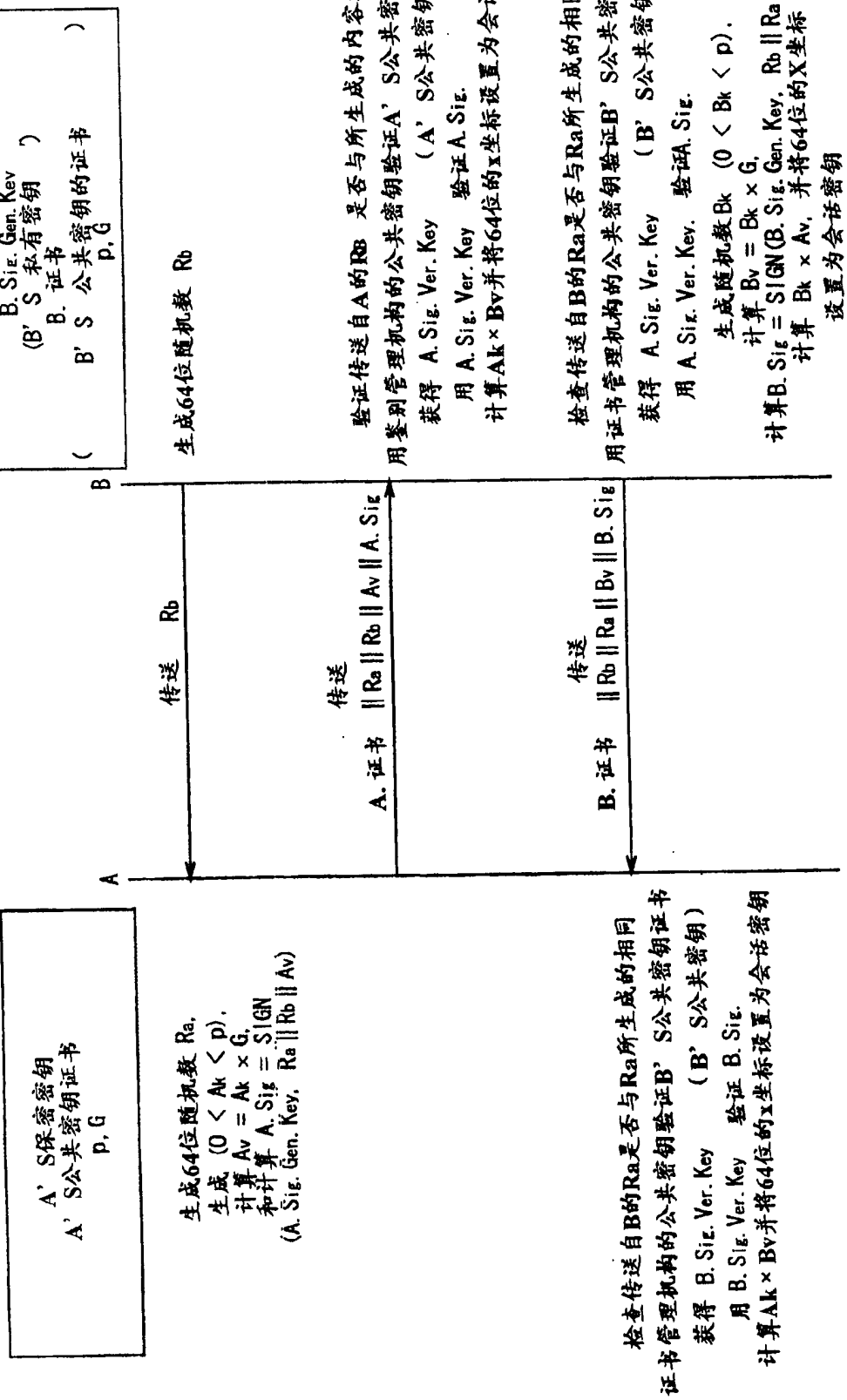
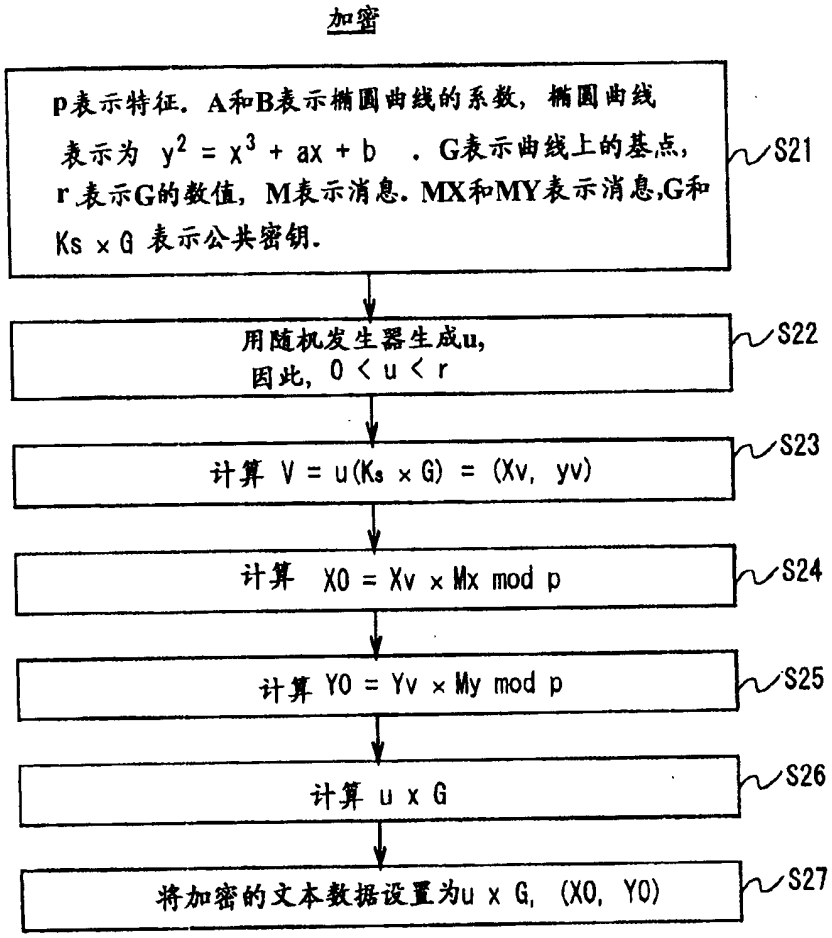


图 15

用对称密钥密码翻译技术的ISO/IEC9798-2相互鉴别和密钥共享方法



用椭圆曲线密码翻译进行加密MENEZES-VANSTONE)

图 16

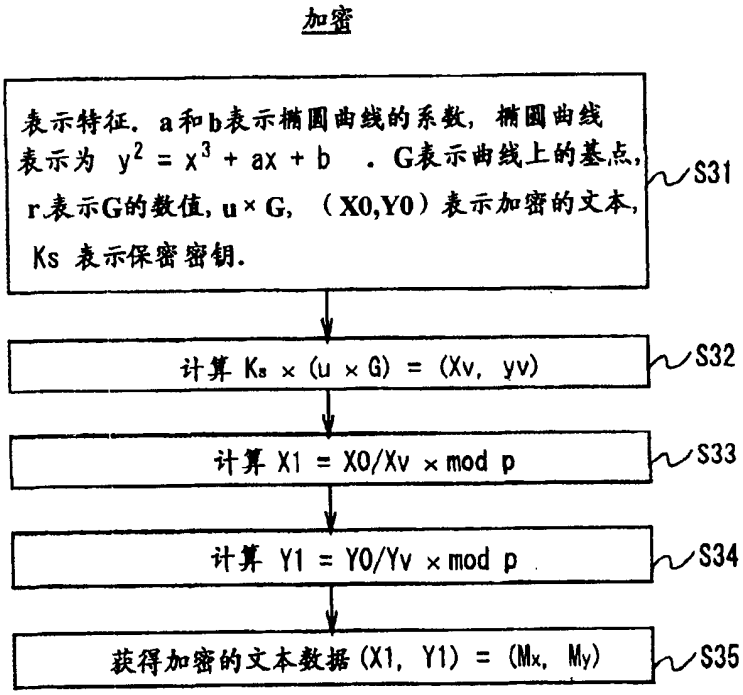

加密
表示特征，a和b表示椭圆曲线的系数，椭圆曲线表示为 $y^2 = x^3 + ax + b$ ．G表示曲线上的基点，r表示G的数值，u × G，（X0,Y0）表示加密的文本，Ks 表示保密密钥．
S31
计算 Ks × (u × G) = (Xv, yv)
S32
计算 X1 = X0/Xv × mod p
S33
计算 Y1 = Y0/Yv × mod p
S34
获得加密的文本数据 (X1, Y1) = (Mx, My)
S35
用椭圆曲线密码翻译进行加密(MENEZES-VANSTONE)

图 17

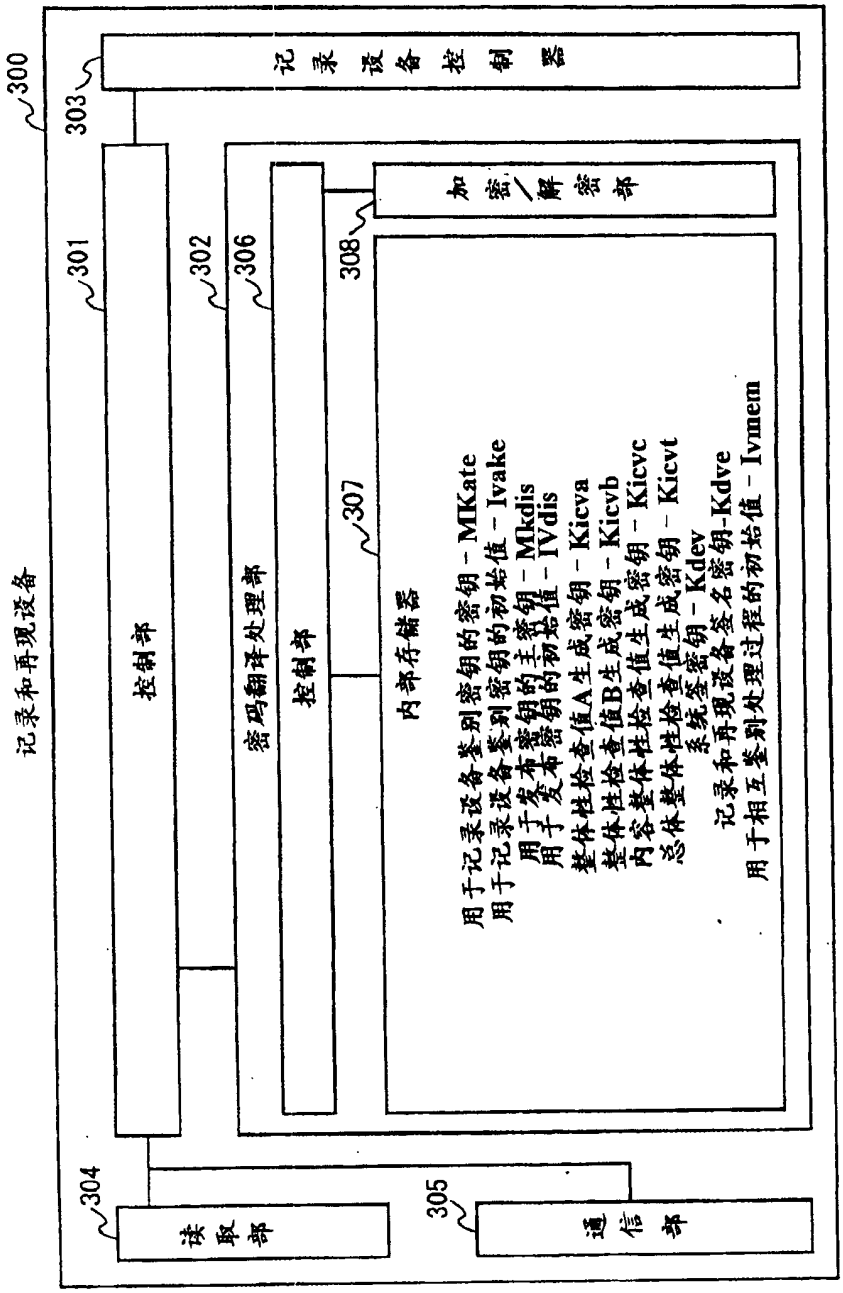


图 18

如何将数据保存在记录和再现设备上

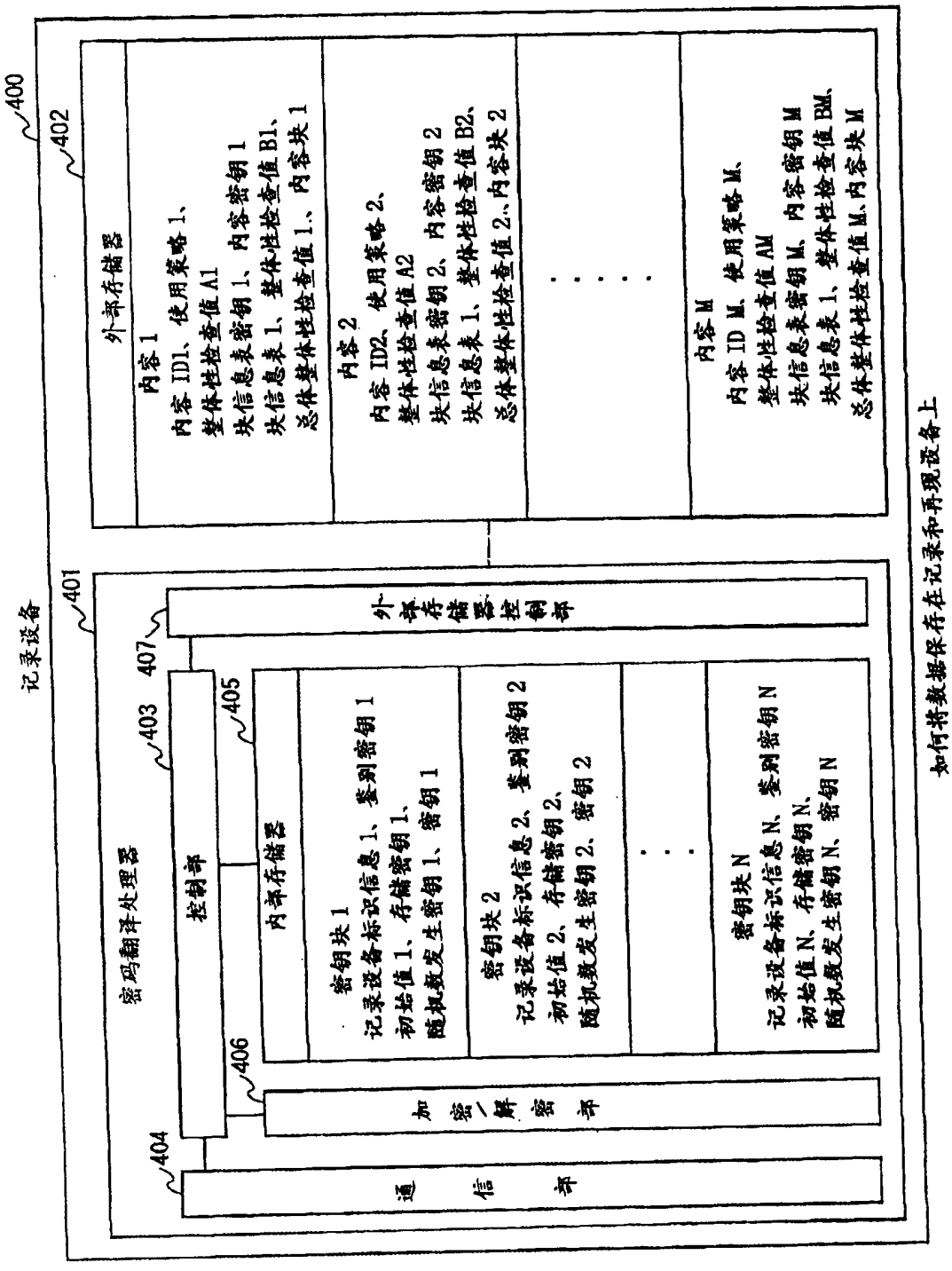
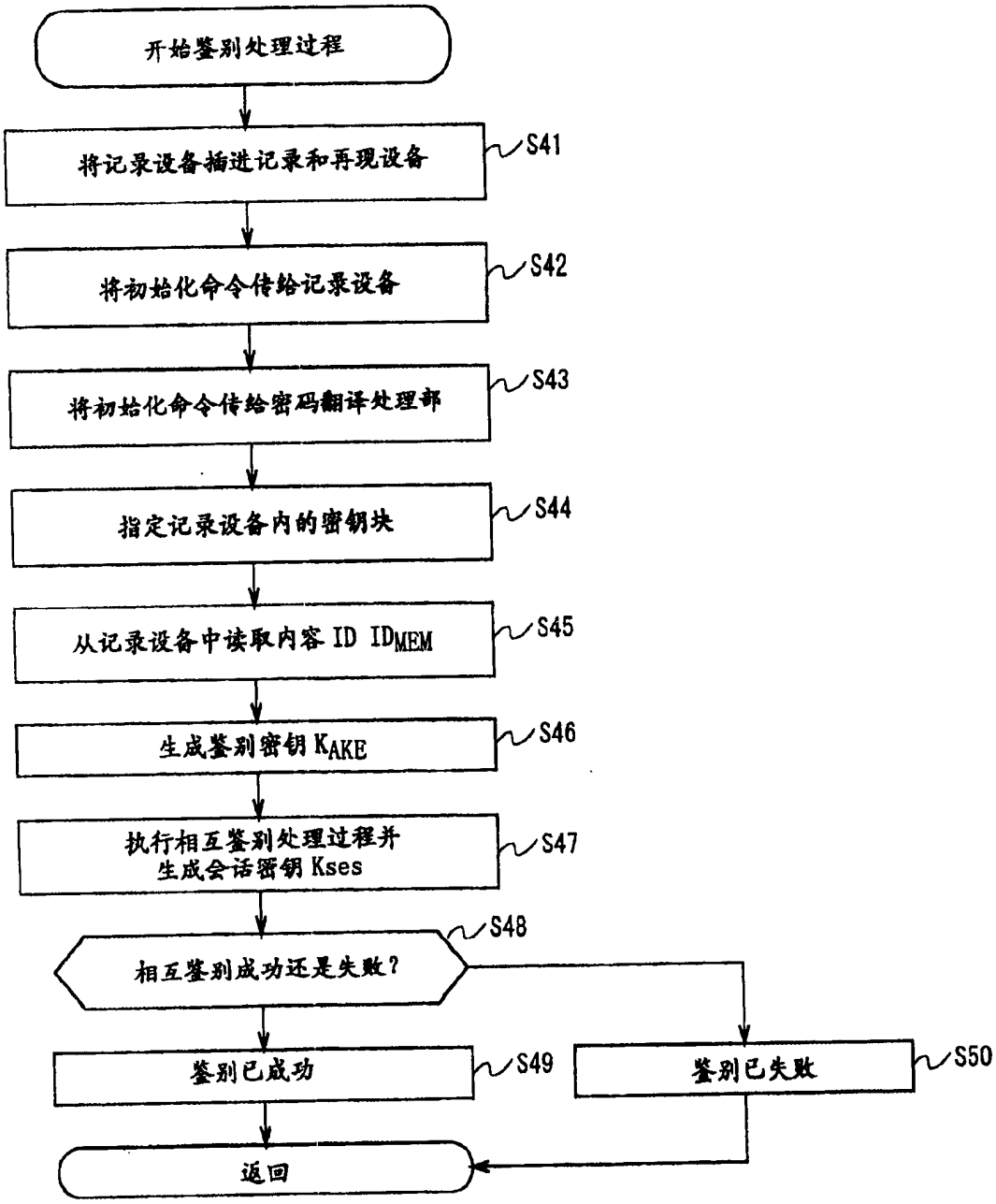


图 19

如何将数据保存在记录和再现设备上



记录和再现设备与记录设备之间的相互鉴别

图 20

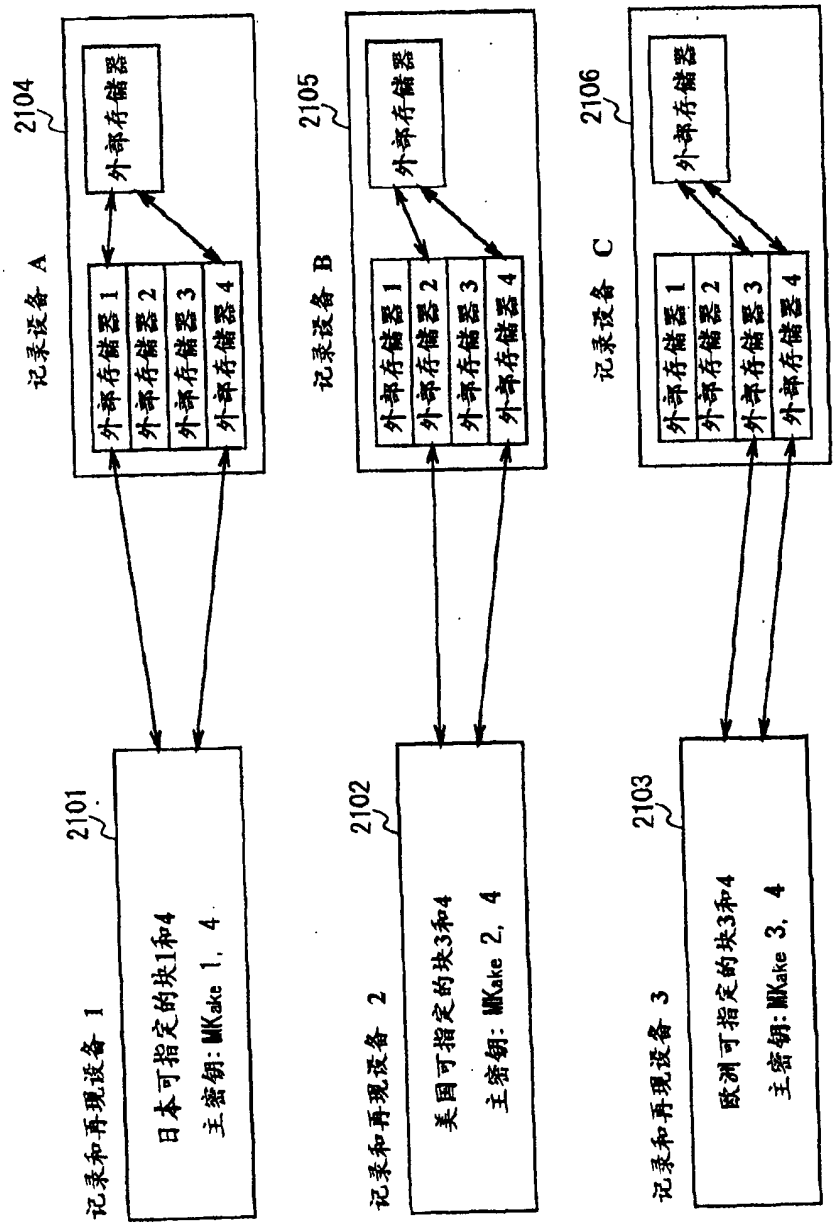
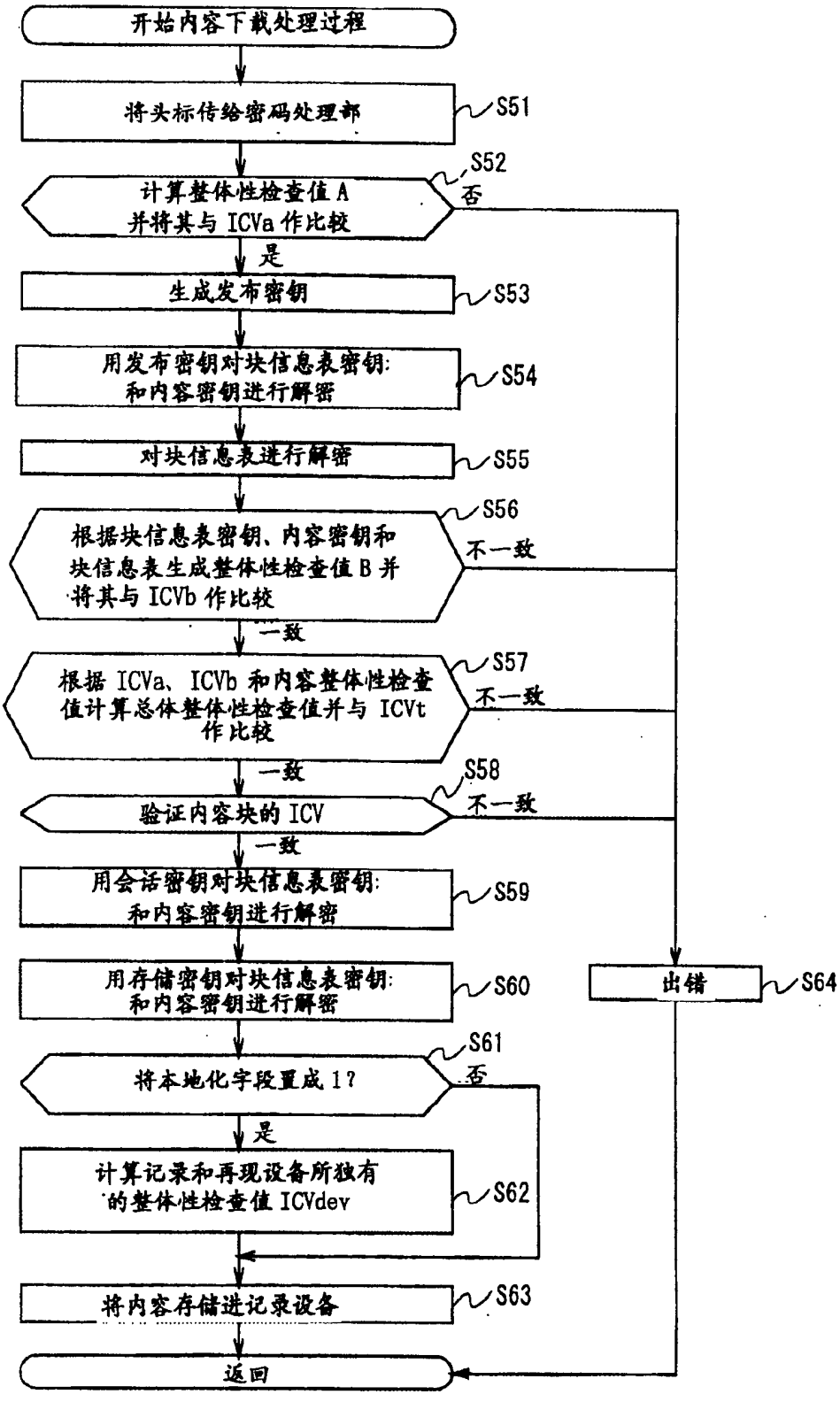
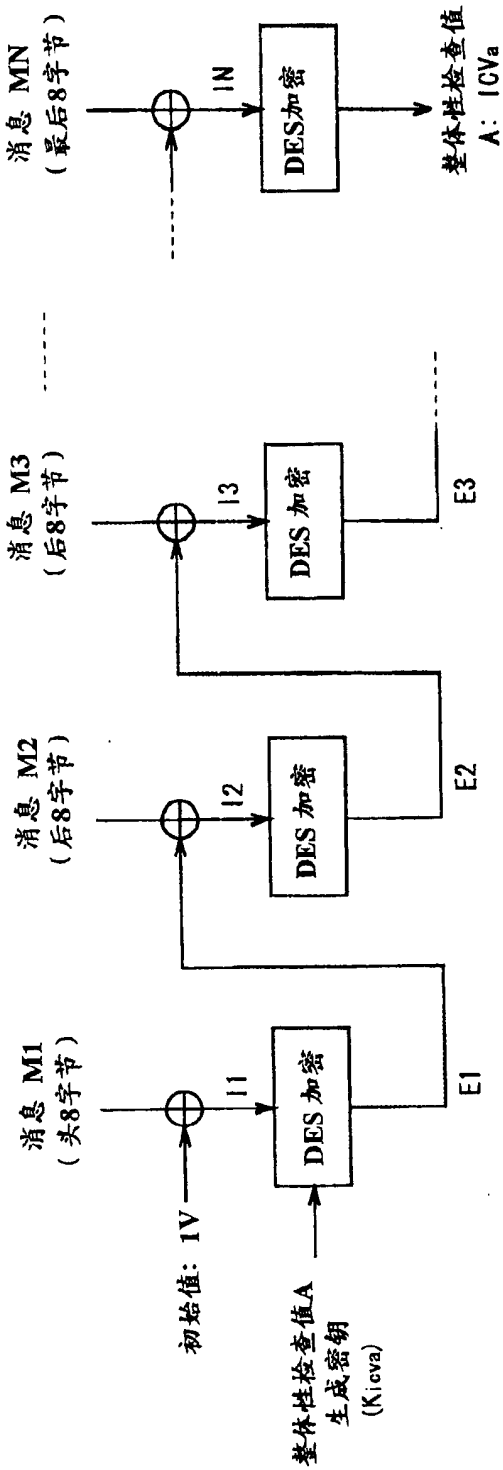

记录设备 A
2104
外部存储器
外部存储器 1
外部存储器 2
外部存储器 3
外部存储器 4
记录和再现设备 1
2101
日本可指定的块1和4
主密钥: MKake 1, 4
记录设备 B
2105
外部存储器
外部存储器 1
外部存储器 2
外部存储器 3
外部存储器 4
记录和再现设备 2
2102
美国可指定的块3和4
主密钥: MKake 2, 4
记录设备 C
2106
外部存储器
外部存储器 1
外部存储器 2
外部存储器 3
外部存储器 4
记录和再现设备 3
2103
欧洲可指定的块3和4
主密钥: MKake 3, 4

图 21



内容下载处理过程

图 22



消息M1至MN：内容ID和使用策略

⊕：异或处理过程（每8字节）

图 23

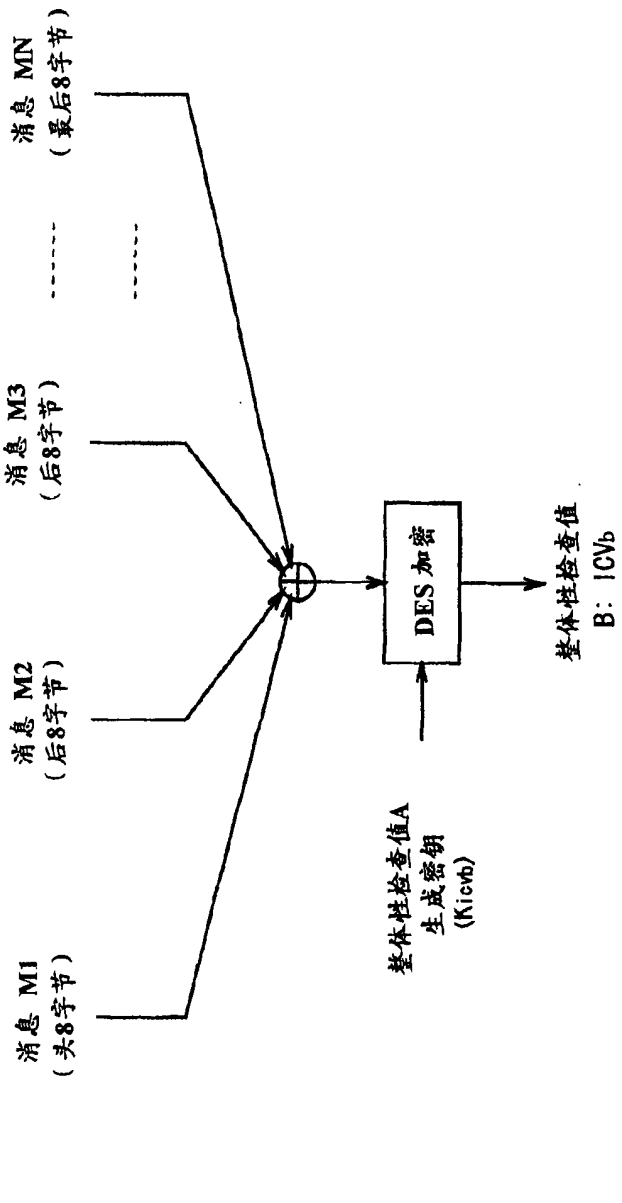

消息 MN
（最后8字节）
消息 M3
（后8字节）
消息 M2
（后8字节）
消息 M1
（头8字节）
整体性检查值A
生成密钥
(Kicvb)
DES 加密
整体性检查值
B: ICVb
消息M1至MN: 块信息表密钥 Kbit, 内容密钥 Kcon, 块信息表
⊕: 异或处理过程（每8字节）

图 24

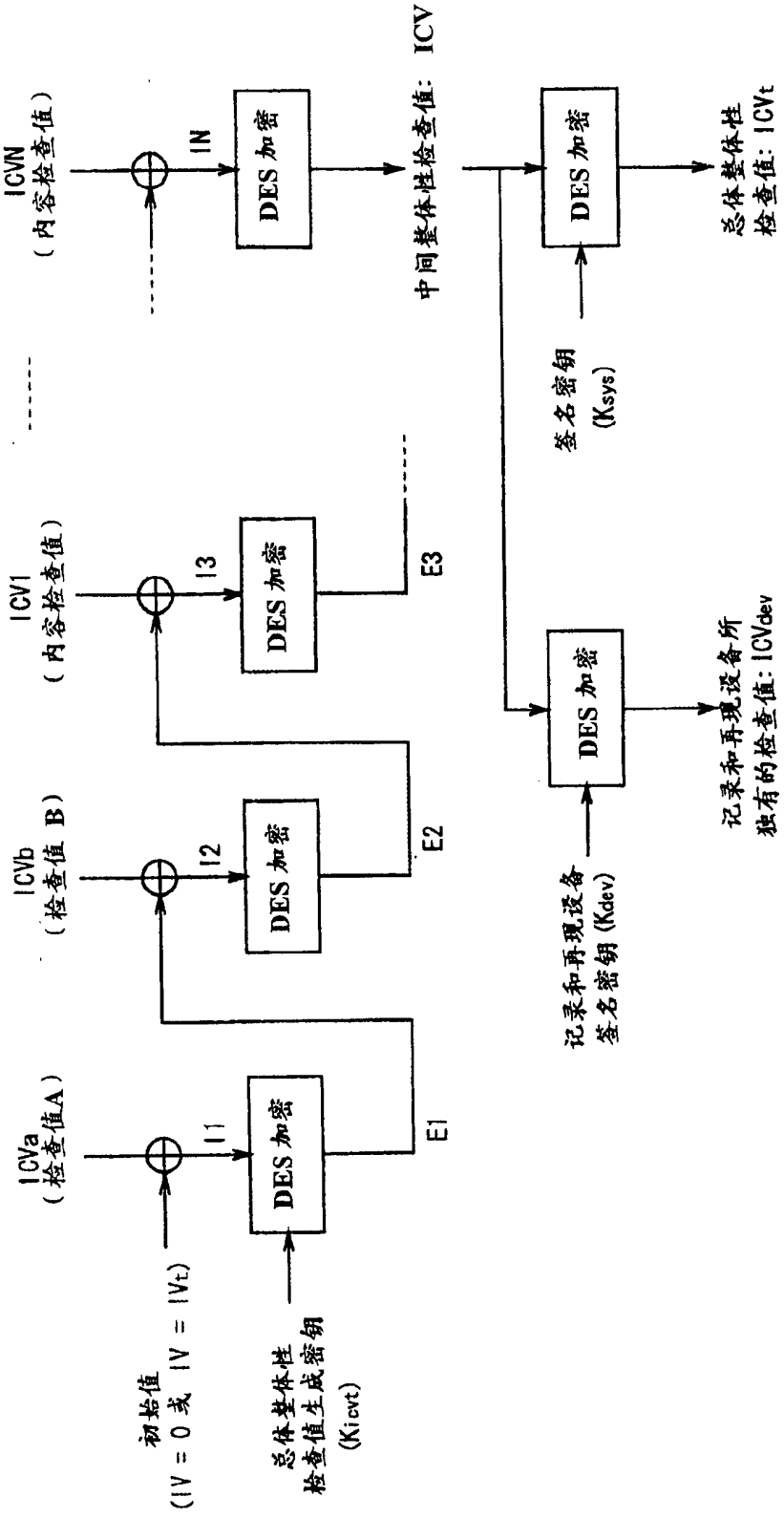

ICVa
(检查值A)
初始值
(IV = 0 或 IV = IVt)
I1
DES 加密
总体整体性
检查值生成密钥
(Kicvt)
E1
ICVb
(检查值 B)
I2
DES 加密
E2
ICV1
(内容检查值)
I3
DES 加密
E3
ICVN
(内容检查值)
IN
DES 加密
中间整体性检查值: ICV
记录和再现设备
签名密钥 (Kdev)
DES 加密
记录和再现设备所
独有的检查值: ICVdev
签名密钥
(Ksys)
DES 加密
总体整体性
检查值: ICVt
⊕: 异或处理过程 (每8字节)

图 25

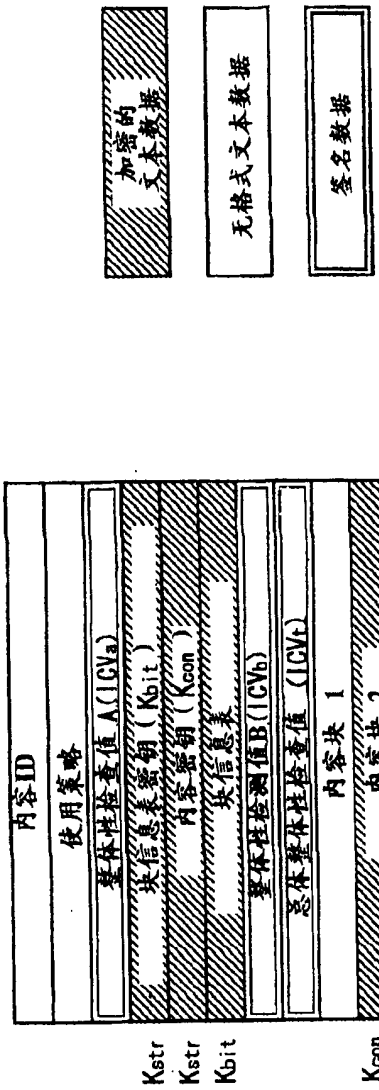

加密的
无格式文本数据
签名数据
内容ID
使用策略
整体性检查值 A(ICVa)
块信息表密钥 (Kbit)
内容密钥 (Kcon)
块信息表
整体性检测值B(ICVb)
总体整体性检查值 (ICVt)
内容块 1
内容块 2
内容块 i
内容块 N
Kstr
Kstr
Kbit
Kcon
Kcon
存储在记录设备中的内容
(位置字段 = 0)

图 26

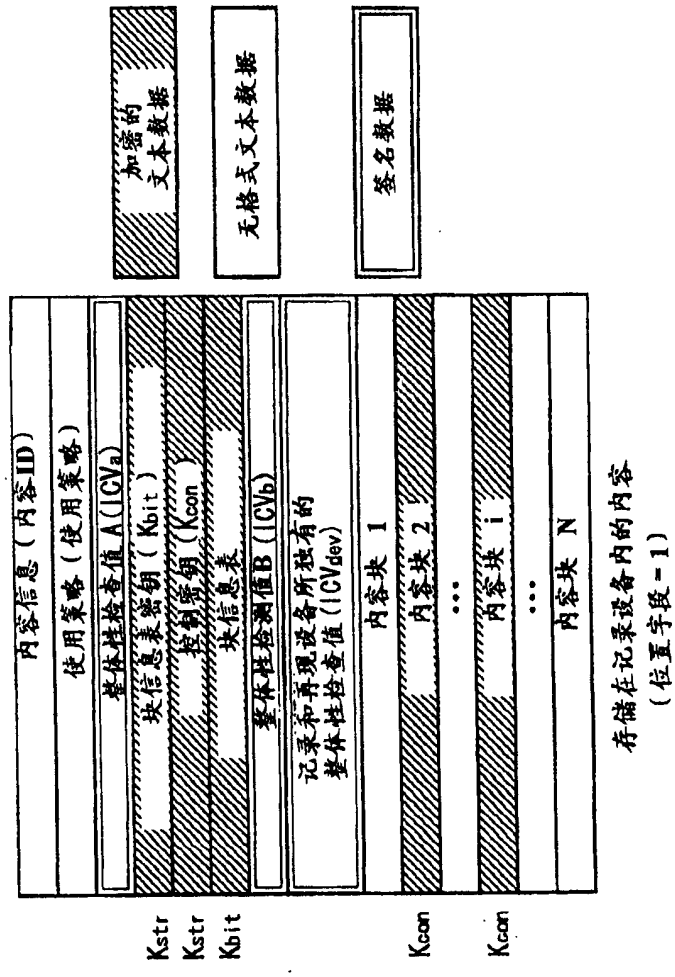

内容信息（内容ID）
使用策略（使用策略）
整体性检查值A（ICVa）
块信息表密钥（Kbit）
控制密钥（Kcon）
块信息表
整体性检测值B（ICVb）
记录和再现设备所独有的
整体性检查值（ICVdev）
内容块 1
内容块 2
...
内容块 i
...
内容块 N
Kstr
Kstr
Kbit
Kcon
Kcon
加密的
文本数据
无格式文本数据
签名数据
存储在记录设备内的内容
（位置字段-1）

图 27

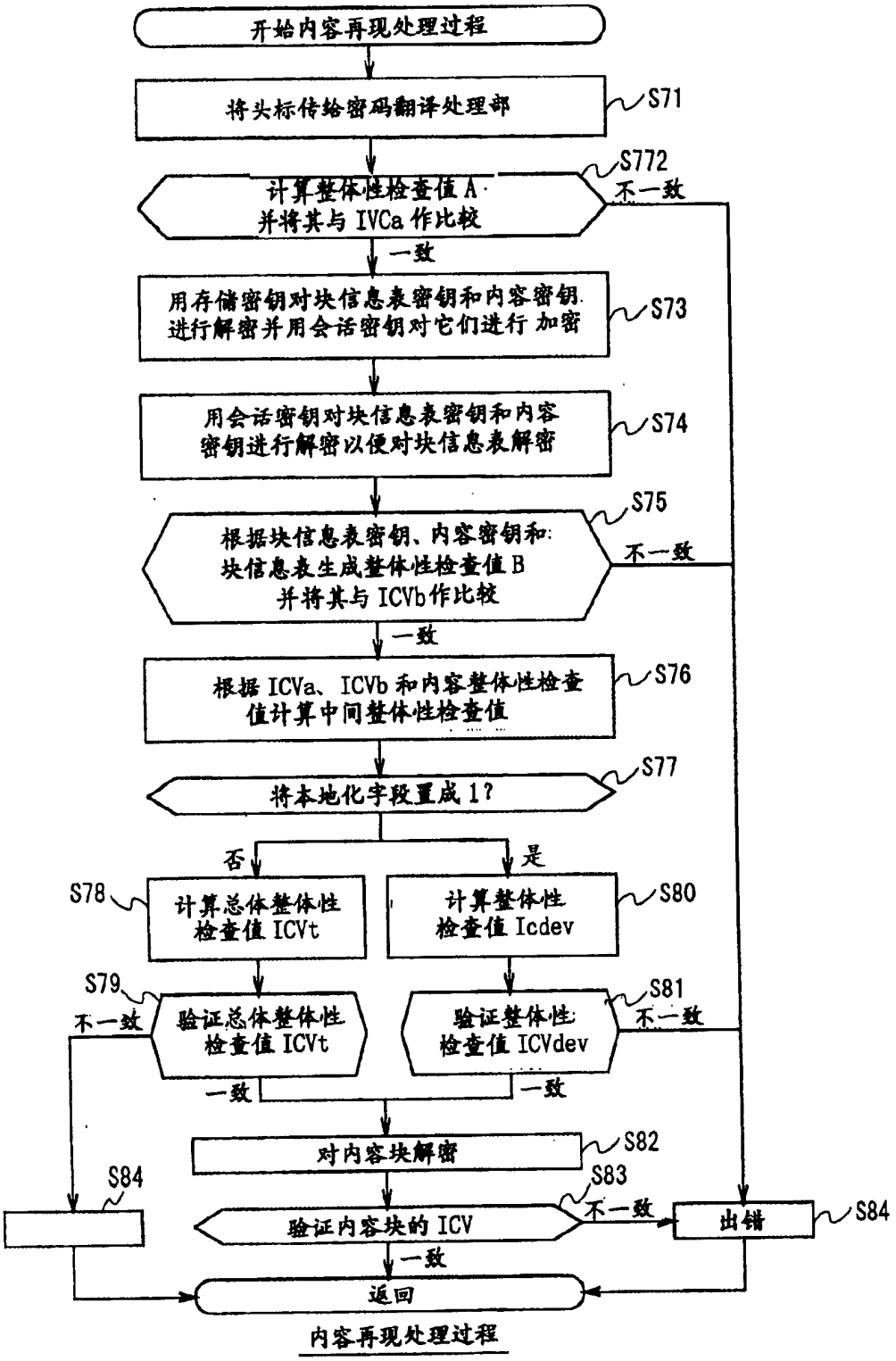

开始内容再现处理过程
将头标传给密码翻译处理部
S71
计算整体性检查值 A
并将其与 IVCa 作比较
S772
不一致
一致
用存储密钥对块信息表密钥和内容密钥
进行解密并用会话密钥对它们进行 加密
S73
用会话密钥对块信息表密钥和内容
密钥进行解密以便对块信息表解密
S74
根据块信息表密钥、内容密钥和
块信息表生成整体性检查值 B
并将其与 ICVb 作比较
S75
不一致
一致
根据 ICVa、ICVb 和内容整体性检查
值计算中间整体性检查值
S76
将本地化字段置成 1?
S77
否
是
计算总体整体性
检查值 ICVt
S78
计算整体性
检查值 Icdev
S80
S79
不一致
验证总体整体性
检查值 ICVt
验证整体性
检查值 ICVdev
S81
不一致
一致
一致
对内容块解密
S82
S84
S83
不一致
验证内容块的 ICV
出错
S84
一致
返回
内容再现处理过程

图 28

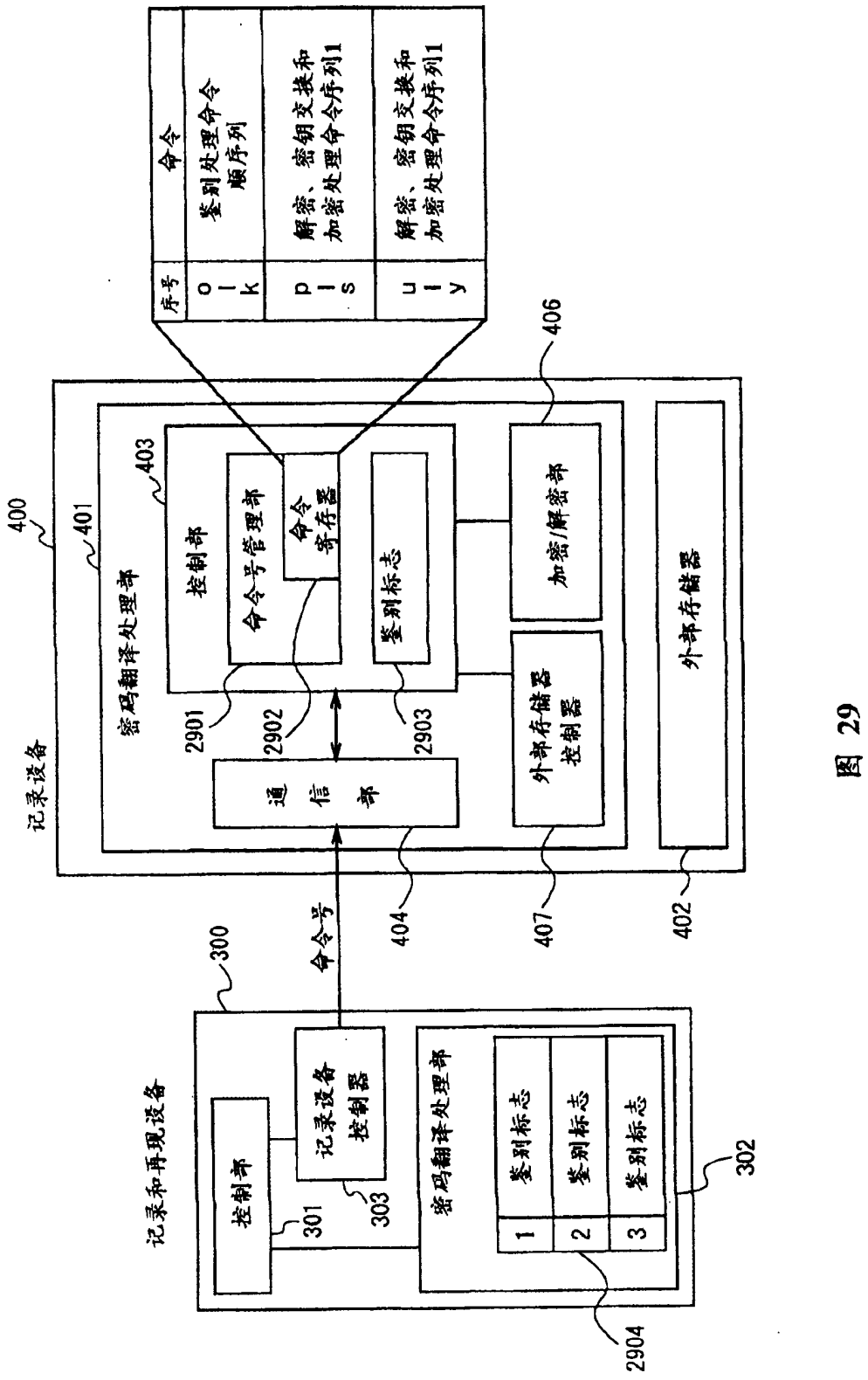

记录和再现设备
记录设备
密码翻译处理部
控制部
记录设备控制器
密码翻译处理部
鉴别标志
鉴别标志
鉴别标志
1
2
3
通信部
外部存储器控制器
加密/解密部
外部存储器
控制部
命令号管理部
命令寄存器
鉴别标志
命令号
300
301
303
302
400
401
403
404
406
407
402
2901
2902
2903
2904
序号
命令
鉴别处理命令顺序列
解密、密钥交换和加密处理命令序列1
解密、密钥交换和加密处理命令序列1
o
l
k
p
l
s
u
l
y

图 29

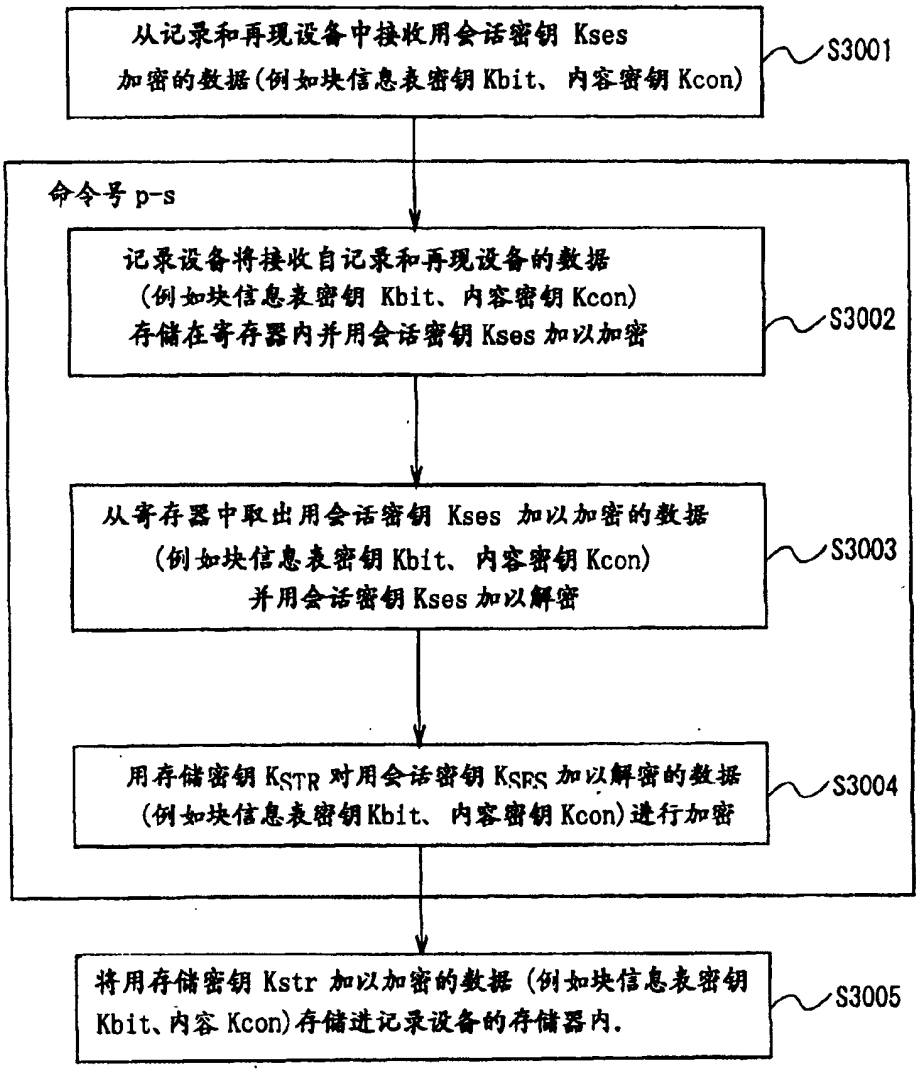

从记录和再现设备中接收用会话密钥 Kses
加密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)
S3001
命令号 p-s
记录设备将接收自记录和再现设备的数据
(例如块信息表密钥 Kbit、内容密钥 Kcon)
存储在寄存器内并用会话密钥 Kses 加以加密
S3002
从寄存器中取出用会话密钥 Kses 加以加密的数据
(例如块信息表密钥 Kbit、内容密钥 Kcon)
并用会话密钥 Kses 加以解密
S3003
用存储密钥 KSTR 对用会话密钥 KSES 加以解密的数据
(例如块信息表密钥 Kbit、内容密钥 Kcon)进行加密
S3004
将用存储密钥 Kstr 加以加密的数据 (例如块信息表密钥
Kbit、内容 Kcon)存储进记录设备的存储器内.
S3005

图 30

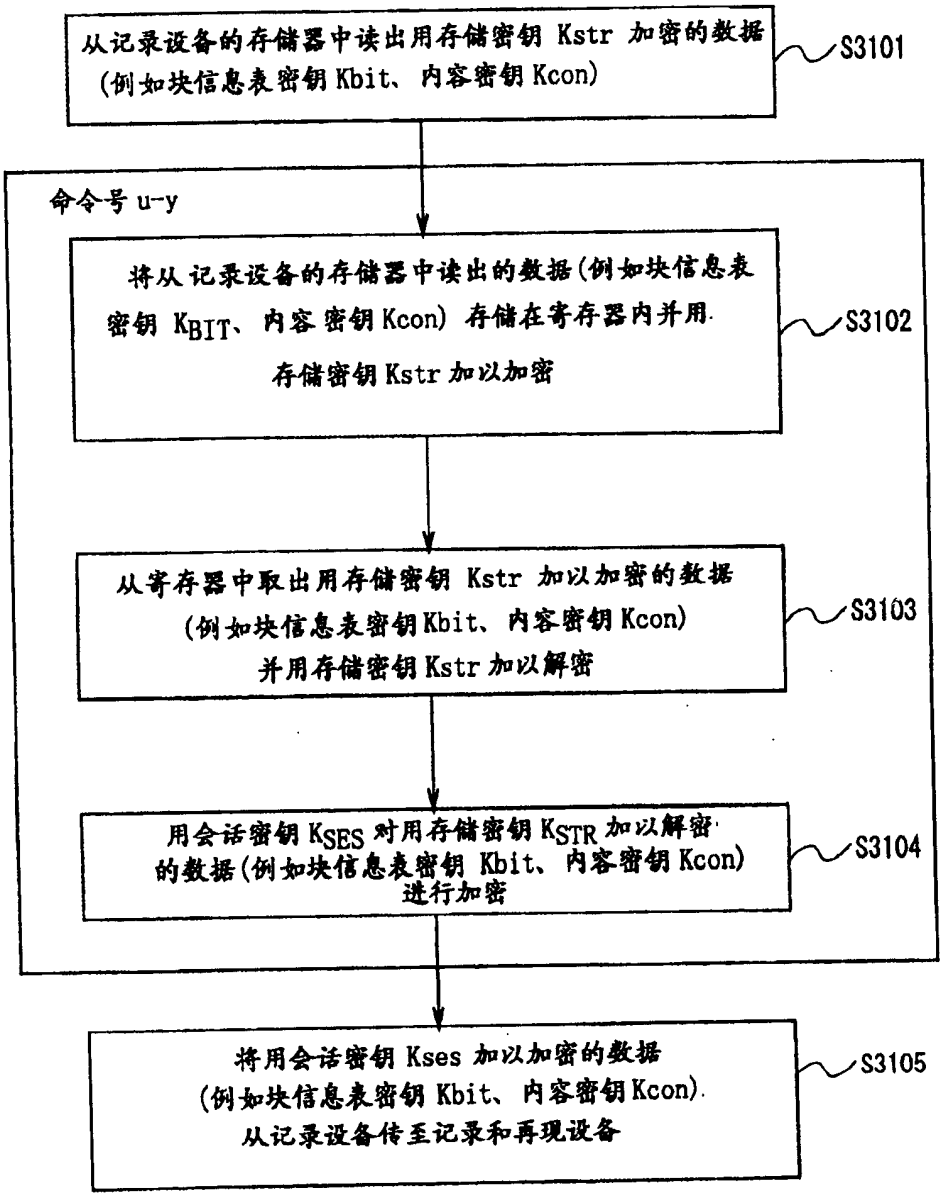

从记录设备的存储器中读出用存储密钥 Kstr 加密的数据
(例如块信息表密钥 Kbit、内容密钥 Kcon)
S3101
命令号 u-y
将从记录设备的存储器中读出的数据(例如块信息表密钥 KBIT、内容密钥 Kcon) 存储在寄存器内并用存储密钥 Kstr 加以加密
S3102
从寄存器中取出用存储密钥 Kstr 加以加密的数据
(例如块信息表密钥 Kbit、内容密钥 Kcon)
并用存储密钥 Kstr 加以解密
S3103
用会话密钥 KSES 对用存储密钥 KSTR 加以解密的数据(例如块信息表密钥 Kbit、内容密钥 Kcon)进行加密
S3104
将用会话密钥 Kses 加以加密的数据
(例如块信息表密钥 Kbit、内容密钥 Kcon)
从记录设备传至记录和再现设备
S3105

图 31

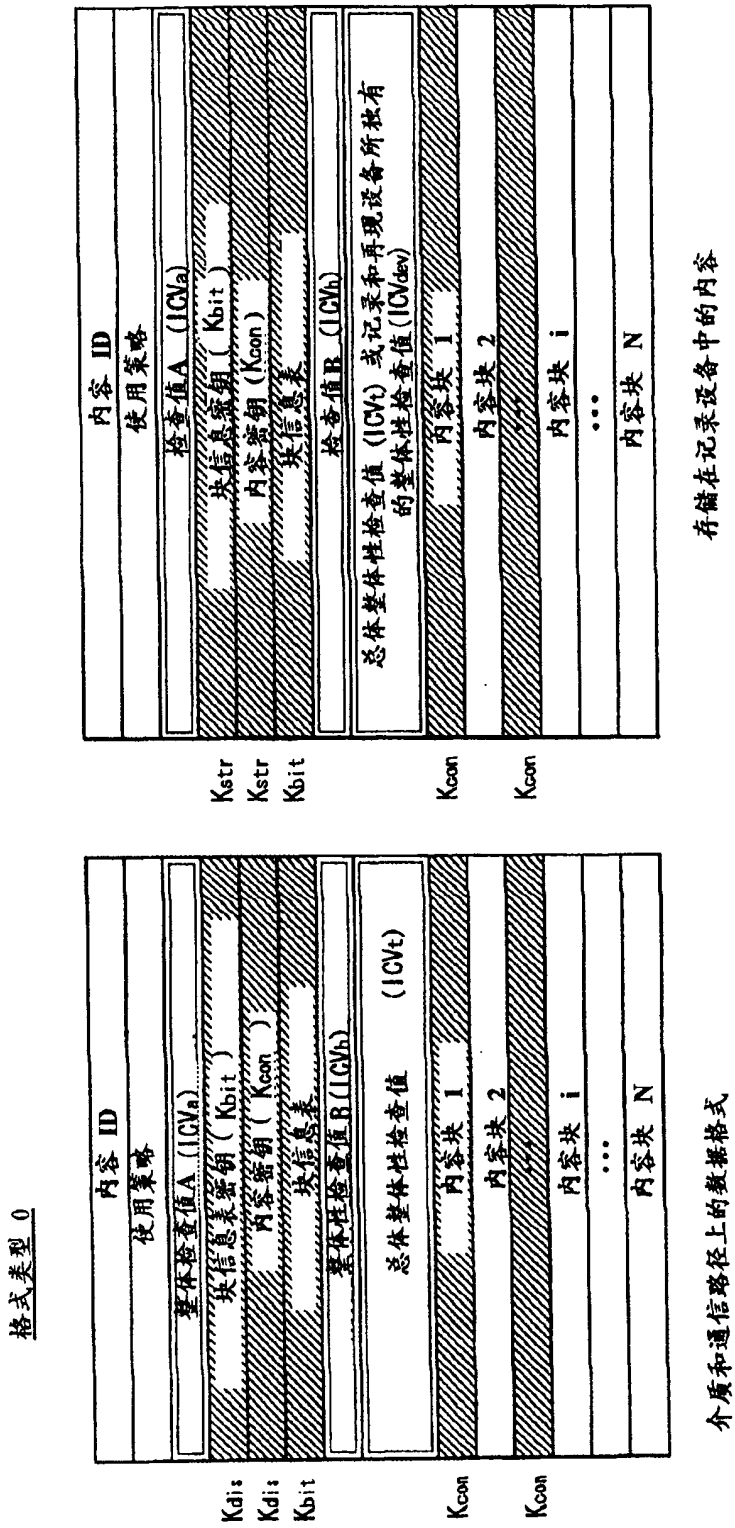

格式类型 0
内容 ID
使用策略
整体检查值A (ICVa)
块信息表密钥 (Kbit)
内容密钥 (Kcon)
块信息表
整体性检查值B (ICVb)
总体整体性检查值 (ICVt)
内容块 1
内容块 2
...
内容块 i
...
内容块 N
Kdis
Kdis
Kbit
Kcon
Kcon
检查值A (ICVa)
块信息表密钥 (Kbit)
内容密钥 (Kcon)
块信息表
检查值B (ICVb)
总体整体性检查值 (ICVt) 或记录和再现设备所拥有的整体性检查值(ICVdev)
内容块 1
内容块 2
...
内容块 i
...
内容块 N
Kstr
Kstr
Kbit
Kcon
Kcon
存储在记录设备中的内容
介质和通信路径上的数据格式
加密的文本数据
无格式文本数据
签名数据

图 32

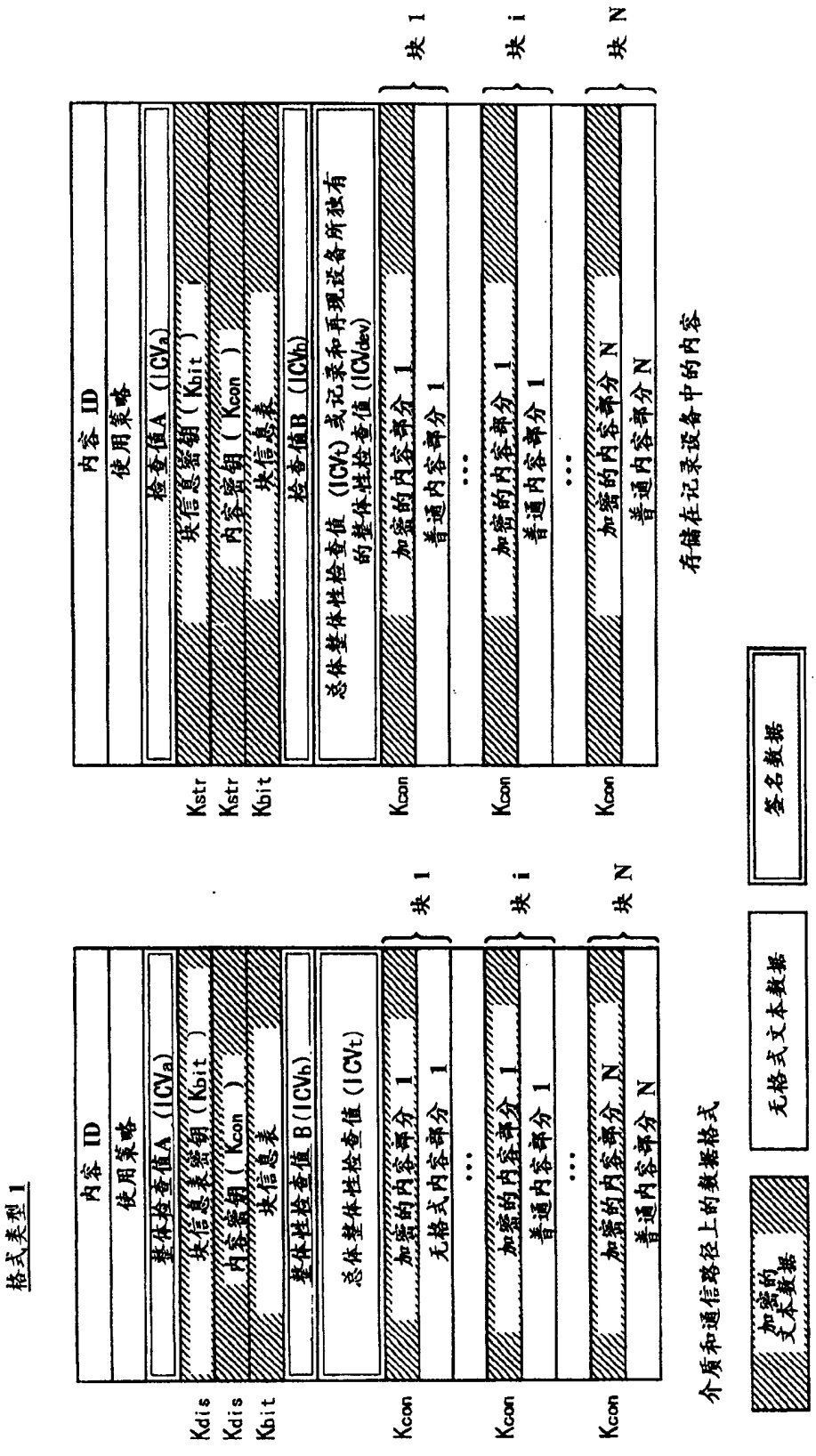

格式类型1
内容 ID
使用策略
整体检查值A (ICVa)
块信息表密钥 (Kbit)
内容密钥 (Kcon)
块信息表
整体性检查值B (ICVb)
总体整体性检查值 (ICVt)
加密的内容部分 1
无格式内容部分 1
加密的内容部分 i
普通内容部分 1
加密的内容部分 N
普通内容部分 N
块 1
块 i
块 N
Kdis
Kbit
Kcon
介质和通信路径上的数据格式
加密的文本数据
无格式文本数据
签名数据
内容 ID
使用策略
检查值A (ICVa)
块信息表密钥 (Kbit)
内容密钥 (Kcon)
块信息表
检查值B (ICVb)
总体整体性检查值 (ICVt) 或记录和再现设备所独有的整体性检查值 (ICVdev)
加密的内容部分 1
普通内容部分 1
加密的内容部分 i
普通内容部分 1
加密的内容部分 N
普通内容部分 N
块 1
块 i
块 N
Kstr
Kbit
Kcon
存储在记录设备中的内容

图 33

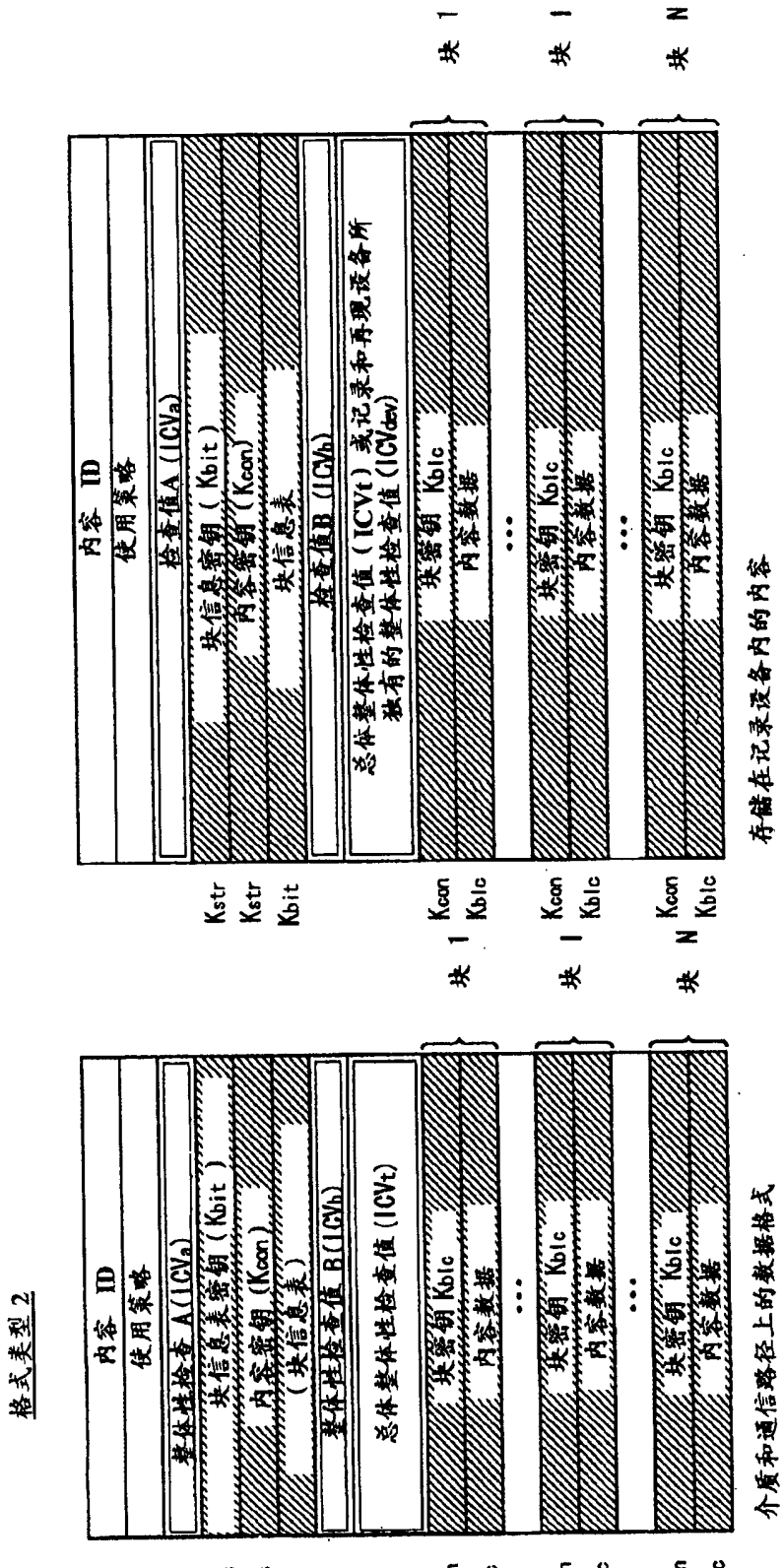

格式类型2
内容 ID
使用策略
整体性检查 A(ICVa)
块信息表密钥(Kbit)
内容密钥(Kcon)
(块信息表)
整体性检查值 B(ICVb)
总体整体性检查值(ICVt)
块密钥 Kblc
内容数据
Kdis
Kdis
Kbit
Kcon
Kblc
块 1
块 I
块 N
介质和通信路径上的数据格式
内容 ID
使用策略
检查值A(ICVa)
块信息表密钥(Kbit)
内容密钥(Kcon)
块信息表
检查值B(ICVb)
总体整体性检查值(ICVt)或记录和再现设备所
独有的整体性检查值(ICVdev)
Kstr
Kstr
Kbit
存储在记录设备内的内容
加密的文本数据
无格式文本数据
签名数据

图 34

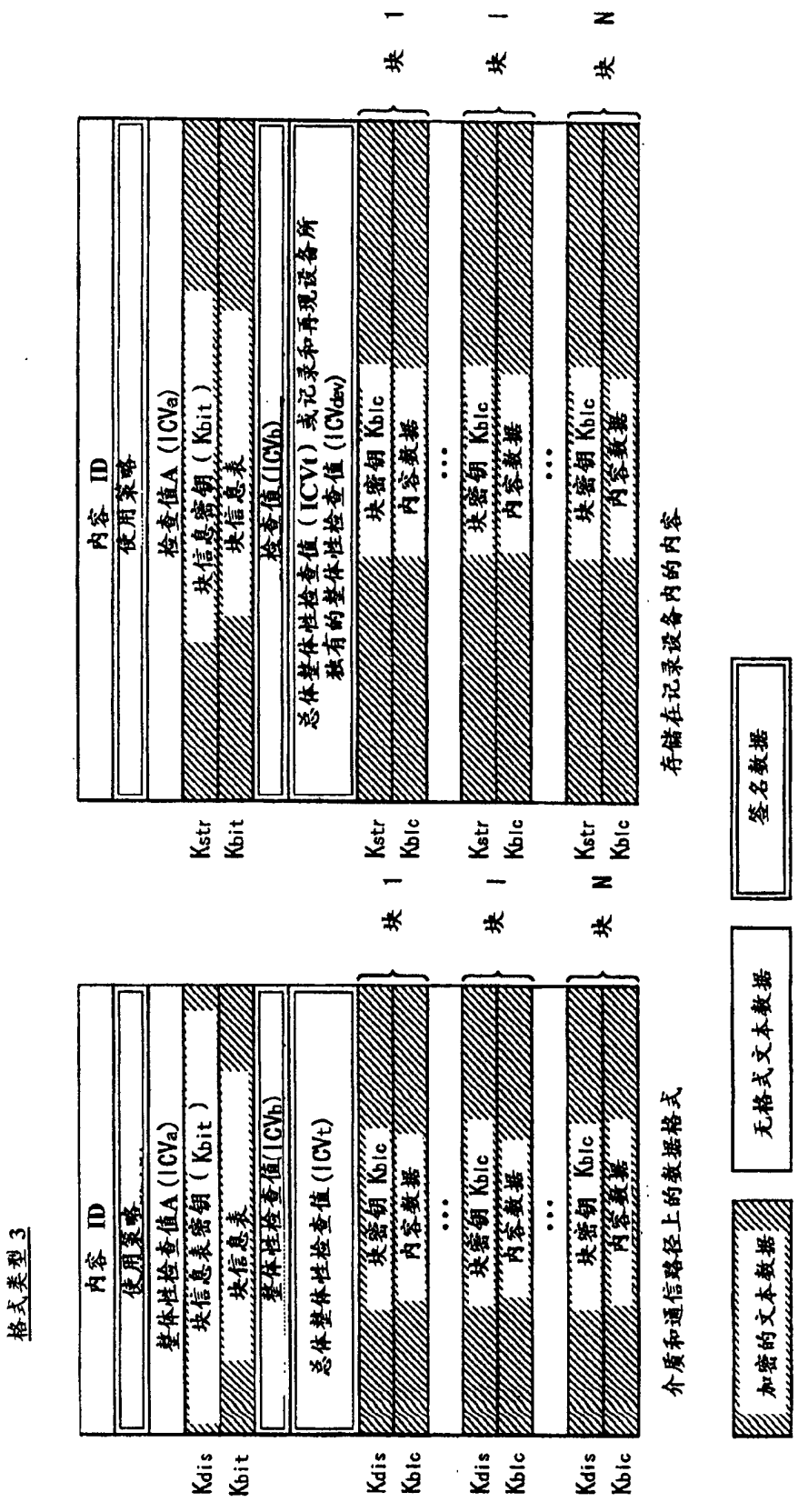

格式类型 3
内容 ID
使用策略
整体性检查值A (ICVa)
块信息表密钥 (Kbit)
块信息表
整体性检查值(ICVb)
总体整体性检查值 (ICVt)
块密钥 Kblc
内容数据
Kdis
Kbit
Kblc
块 1
块 I
块 N
介质和通信路径上的数据格式
内容 ID
使用策略
检查值A (ICVa)
块信息密钥 (Kbit)
块信息表
检查值(ICVb)
总体整体性检查值 (ICVt) 或记录和再现设备所
获有的整体性检查值 (ICVdev)
块密钥 Kblc
内容数据
Kstr
Kbit
Kblc
块 1
块 I
块 N
存储在记录设备内的内容
加密的文本数据
无格式文本数据
签名数据

图 35

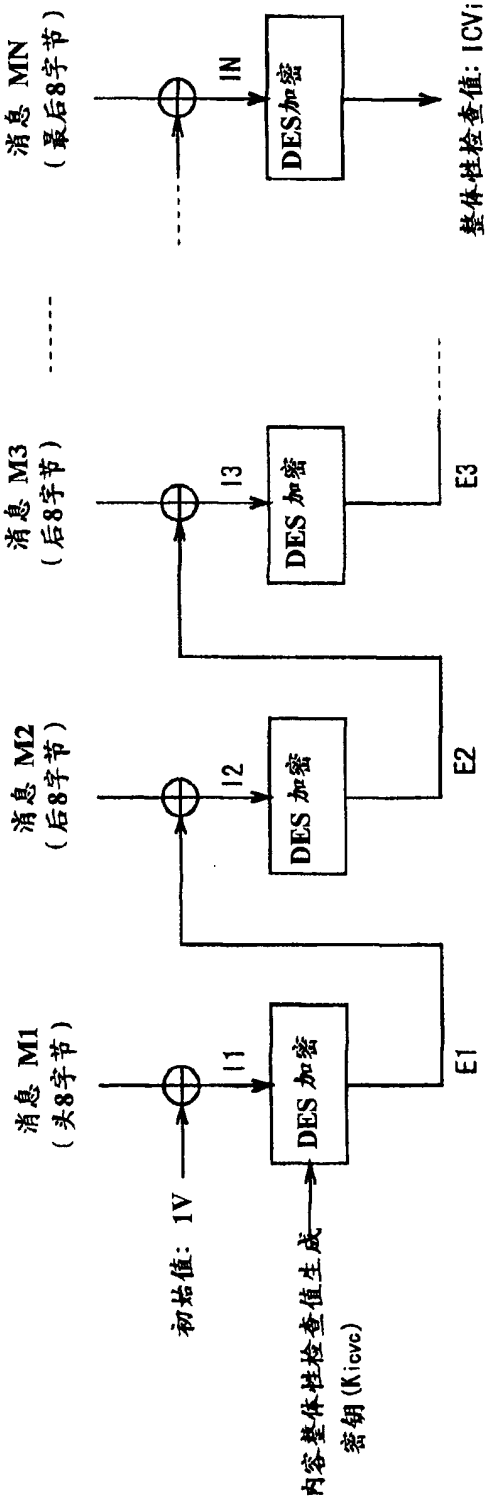

消息 M1
（头8字节）
消息 M2
（后8字节）
消息 M3
（后8字节）
消息 MN
（最后8字节）
初始值：IV
I1
I2
I3
IN
DES 加密
DES 加密
DES 加密
DES加密
E1
E2
E3
整体性检查值：ICVi
内容整体性检查值生成
密钥 (Kicvc)
消息M1至MN：内容i中的内容数据
⊕：异或处理过程（每8字节）

图 36

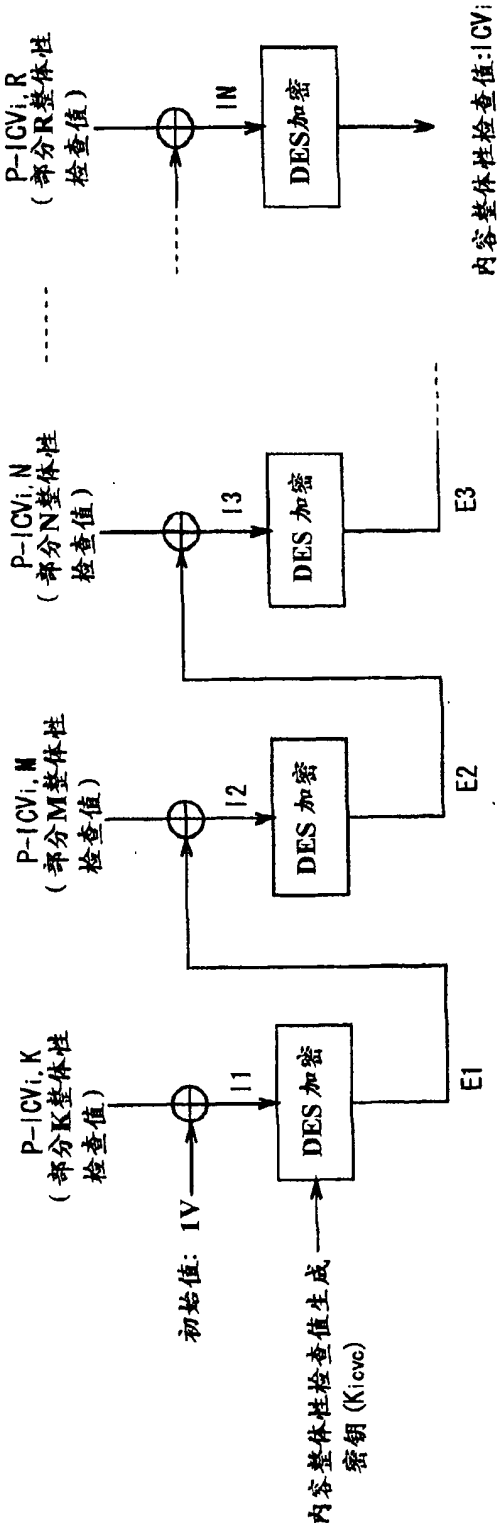

初始值: IV
内容整体性检查值生成密钥 (K_{icvc})
P-ICV$_i$, K (部分K整体性检查值)
P-ICV$_i$, M (部分M整体性检查值)
P-ICV$_i$, N (部分N整体性检查值)
P-ICV$_i$, R (部分R整体性检查值)
I1
I2
I3
IN
DES加密
E1
E2
E3
内容整体性检查值:ICV$_i$
⊕: 异或处理过程 (每8字节)

图 37

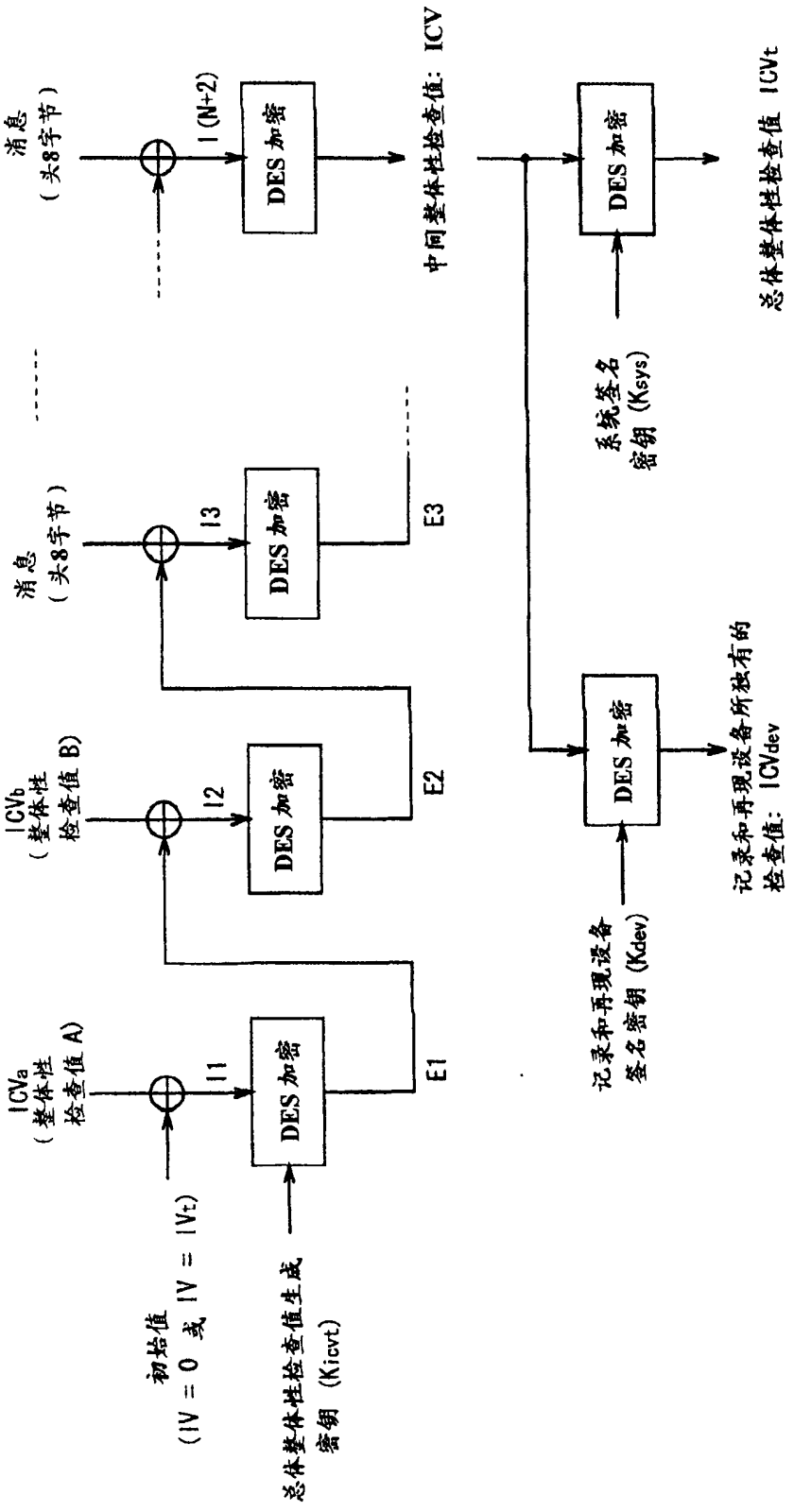

ICVa
(整体性
检查值 A)
初始值
(IV = 0 或 IV = IVt)
I1
DES 加密
总体整体性检查值生成
密钥 (Kicvt)
E1
ICVb
(整体性
检查值 B)
I2
DES 加密
E2
消息
(共8字节)
I3
DES 加密
E3
消息
(共8字节)
I (N+2)
DES 加密
中间整体性检查值: ICV
记录和再现设备
签名密钥 (Kdev)
DES 加密
记录和再现设备所独有的
检查值: ICVdev
系统签名
密钥 (Ksys)
DES 加密
总体整体性检查值 ICVt
消息M1至MN: 内容块1至N中的数据
⊕: 异或处理过程 (每8字节)

图 38

格式类型 0 至 1 下载处理过程

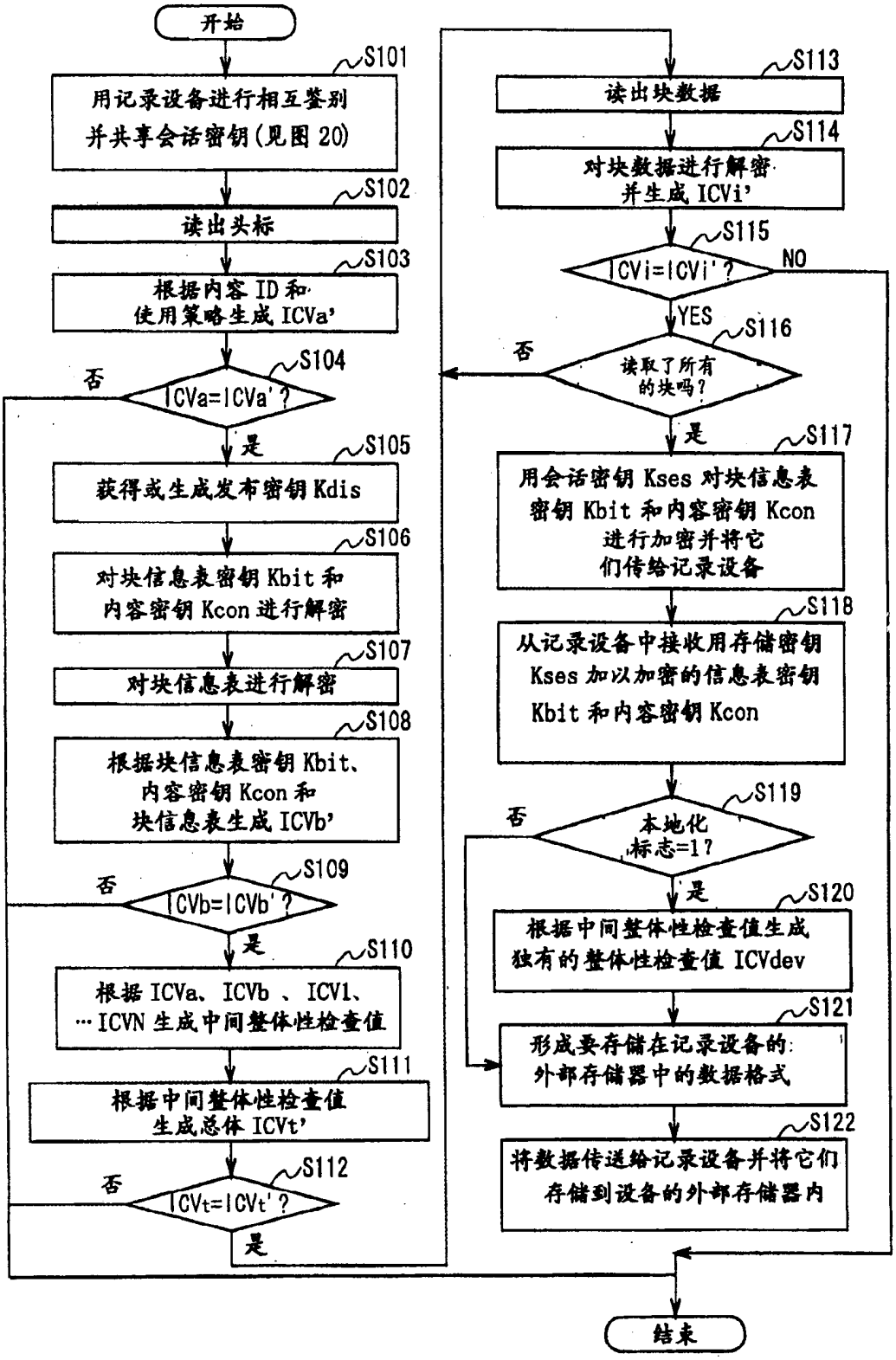


图 39

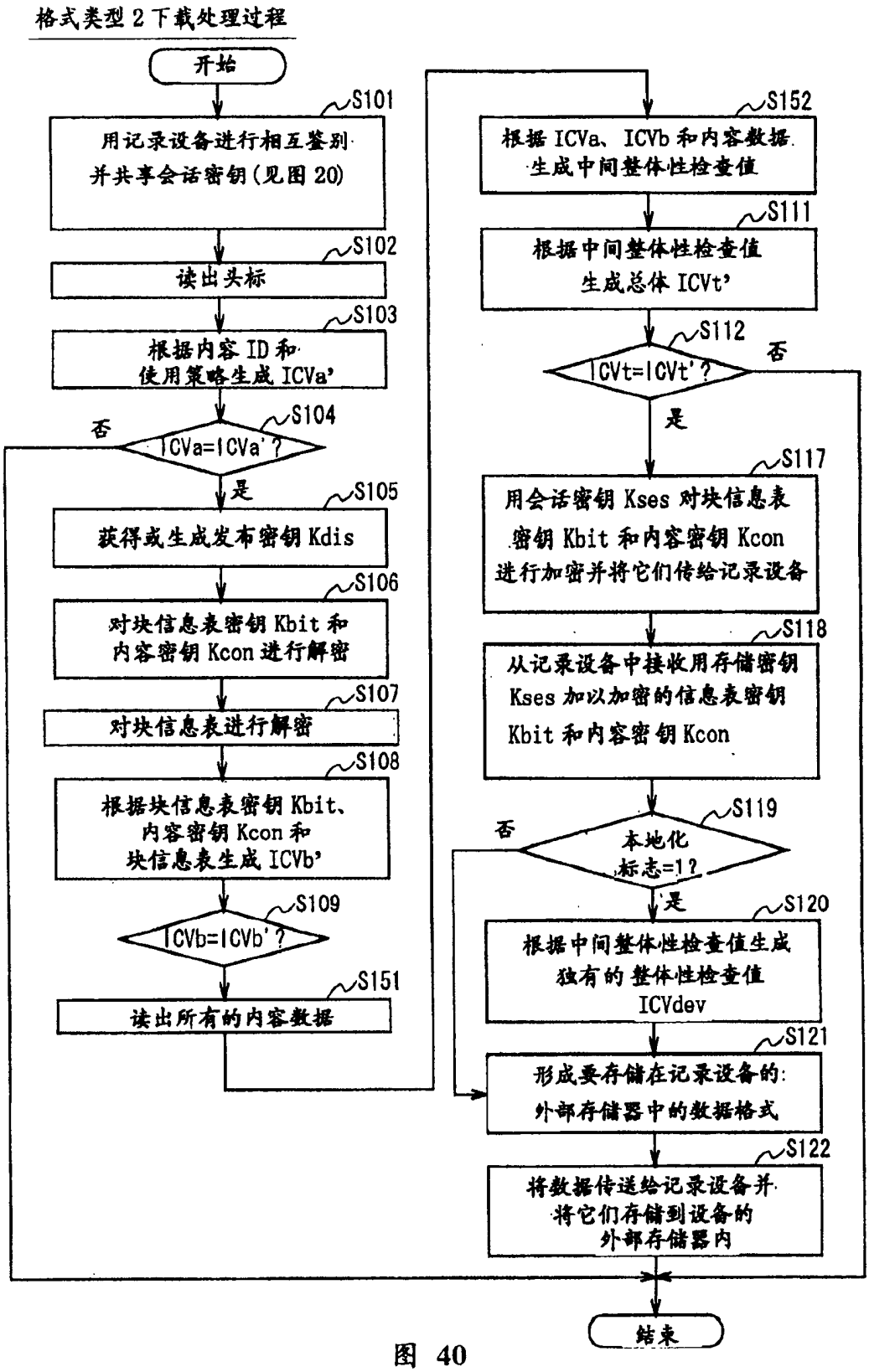

格式类型 2 下载处理过程
开始
S101
用记录设备进行相互鉴别
并共享会话密钥(见图 20)
S102
读出头标
S103
根据内容 ID 和
使用策略生成 ICVa'
S104
否
ICVa=ICVa'?
是
S105
获得或生成发布密钥 Kdis
S106
对块信息表密钥 Kbit 和
内容密钥 Kcon 进行解密
S107
对块信息表进行解密
S108
根据块信息表密钥 Kbit、
内容密钥 Kcon 和
块信息表生成 ICVb'
S109
ICVb=ICVb'?
S151
读出所有的内容数据
S152
根据 ICVa、ICVb 和内容数据
生成中间整体性检查值
S111
根据中间整体性检查值
生成总体 ICVt'
S112
否
ICVt=ICVt'?
是
S117
用会话密钥 Kses 对块信息表
密钥 Kbit 和内容密钥 Kcon
进行加密并将它们传给记录设备
S118
从记录设备中接收用存储密钥
Kses 加以加密的信息表密钥
Kbit 和内容密钥 Kcon
S119
否
本地化
标志=1?
是
S120
根据中间整体性检查值生成
独有的整体性检查值
ICVdev
S121
形成要存储在记录设备的
外部存储器中的数据格式
S122
将数据传送给记录设备并
将它们存储到设备的
外部存储器内
结束

图 40

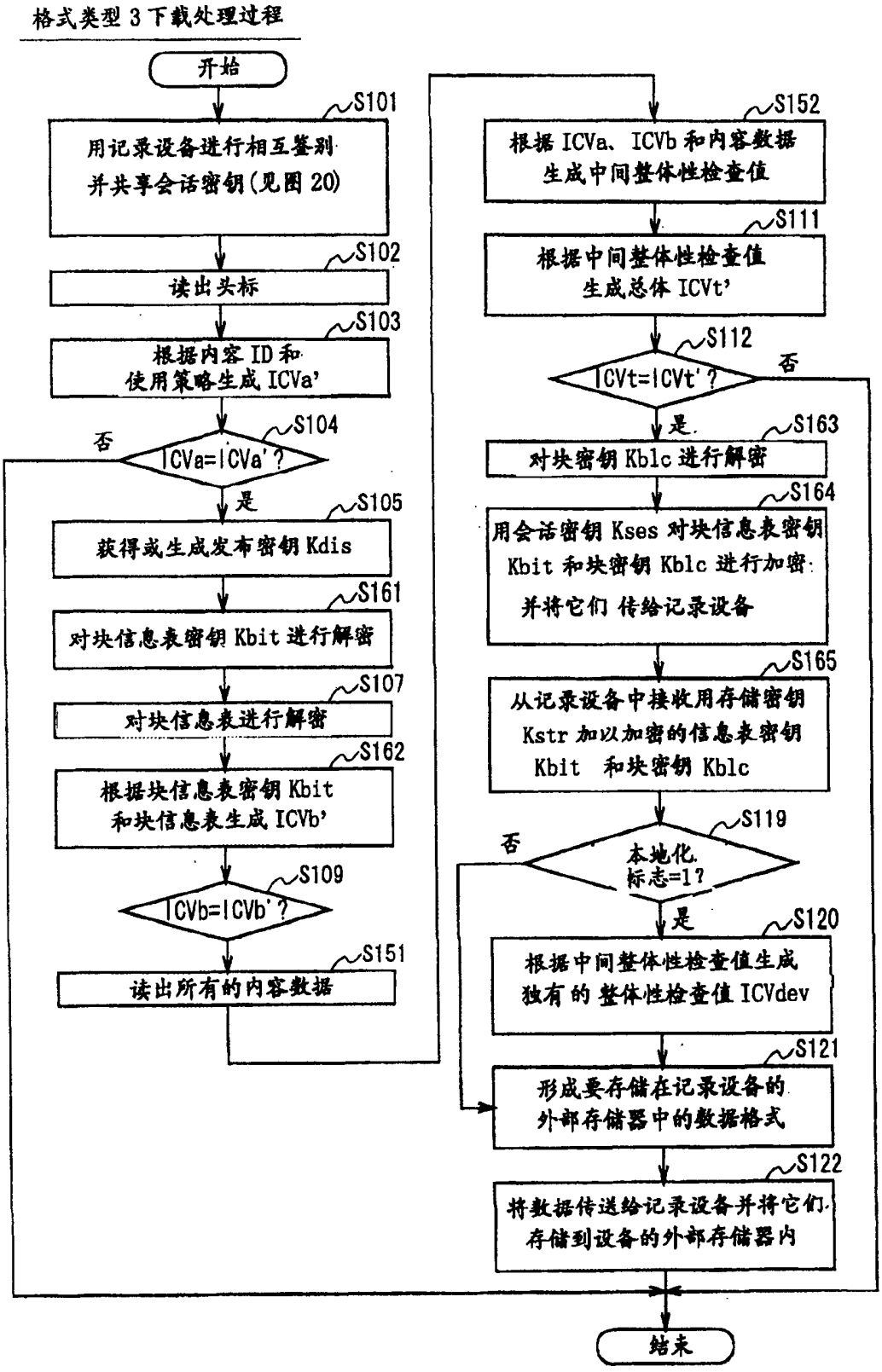

格式类型 3 下载处理过程
开始
S101
用记录设备进行相互鉴别并共享会话密钥(见图 20)
S102
读出头标
S103
根据内容 ID 和使用策略生成 ICVa'
S104
否
ICVa=ICVa'?
是
S105
获得或生成发布密钥 Kdis
S161
对块信息表密钥 Kbit 进行解密
S107
对块信息表进行解密
S162
根据块信息表密钥 Kbit 和块信息表生成 ICVb'
S109
ICVb=ICVb'?
S151
读出所有的内容数据
S152
根据 ICVa、ICVb 和内容数据生成中间整体性检查值
S111
根据中间整体性检查值生成总体 ICVt'
S112
ICVt=ICVt'?
否
是
S163
对块密钥 Kblc 进行解密
S164
用会话密钥 Kses 对块信息表密钥 Kbit 和块密钥 Kblc 进行加密并将它们 传给记录设备
S165
从记录设备中接收用存储密钥 Kstr 加以加密的信息表密钥 Kbit 和块密钥 Kblc
S119
否
本地化标志=1?
是
S120
根据中间整体性检查值生成独有的整体性检查值 ICVdev
S121
形成要存储在记录设备的外部存储器中的数据格式
S122
将数据传送给记录设备并将它们存储到设备的外部存储器内
结束

图 41

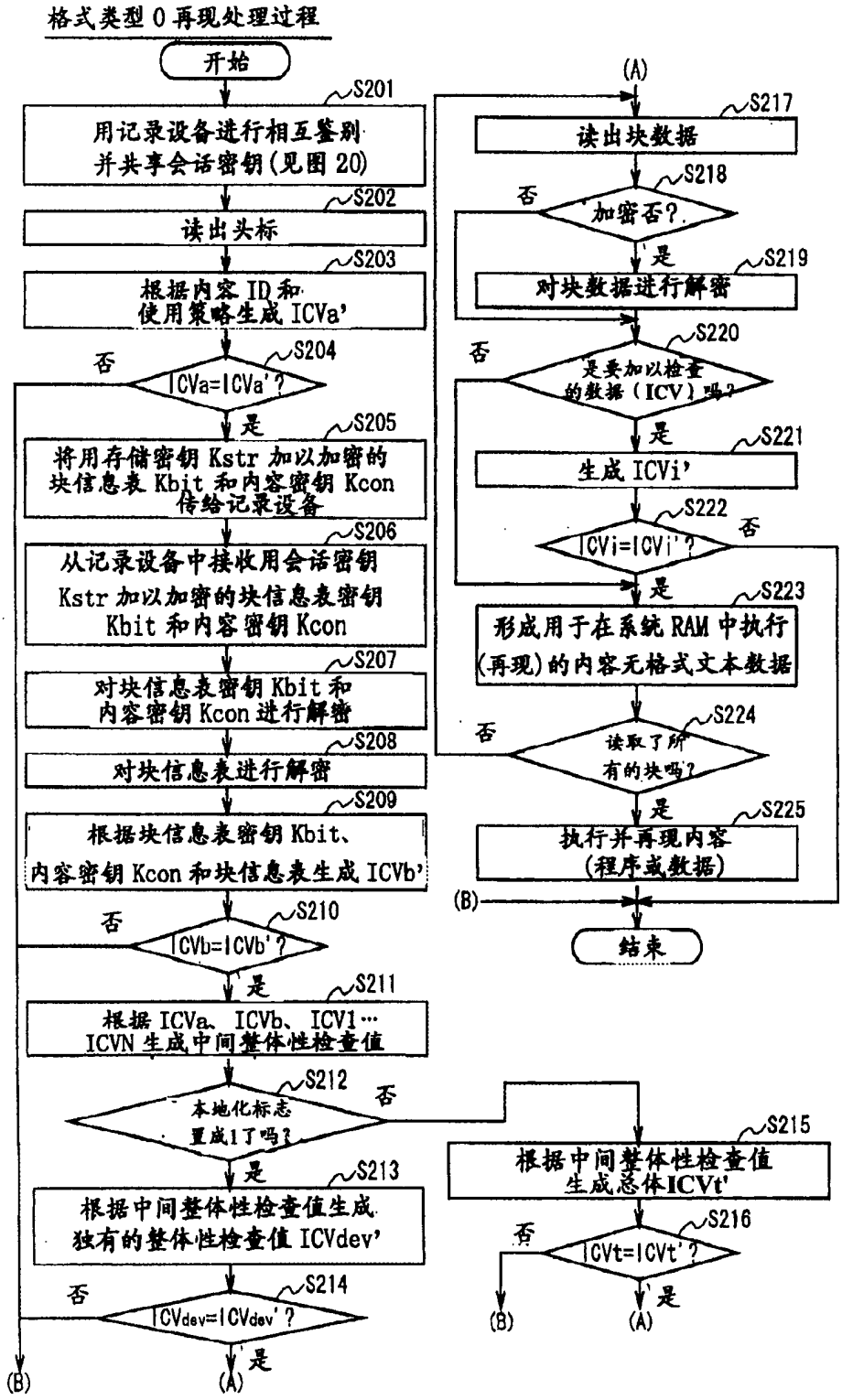

格式类型 0 再现处理过程
开始
S201
用记录设备进行相互鉴别并共享会话密钥(见图 20)
S202
读出头标
S203
根据内容 ID 和使用策略生成 ICVa'
S204
ICVa=ICVa'?
否
是
S205
将用存储密钥 Kstr 加以加密的块信息表 Kbit 和内容密钥 Kcon 传给记录设备
S206
从记录设备中接收用会话密钥 Kstr 加以加密的块信息表密钥 Kbit 和内容密钥 Kcon
S207
对块信息表密钥 Kbit 和内容密钥 Kcon 进行解密
S208
对块信息表进行解密
S209
根据块信息表密钥 Kbit、内容密钥 Kcon 和块信息表生成 ICVb'
S210
ICVb=ICVb'?
否
是
S211
根据 ICVa、ICVb、ICV1… ICVN 生成中间整体性检查值
S212
本地化标志置成1了吗?
否
是
S213
根据中间整体性检查值生成独有的整体性检查值 ICVdev'
S214
ICVdev=ICVdev'?
否
是
(B)
(A)
(A)
S217
读出块数据
S218
加密否?
否
是
S219
对块数据进行解密
S220
是要加以检查的数据(ICV)吗?
否
是
S221
生成 ICVi'
S222
ICVi=ICVi'?
否
是
S223
形成用于在系统 RAM 中执行(再现)的内容无格式文本数据
S224
读取了所有的块吗?
否
是
S225
执行并再现内容(程序或数据)
(B)
结束
S215
根据中间整体性检查值生成总体ICVt'
S216
ICVt=ICVt'?
否
是
(B)
(A)

图 42

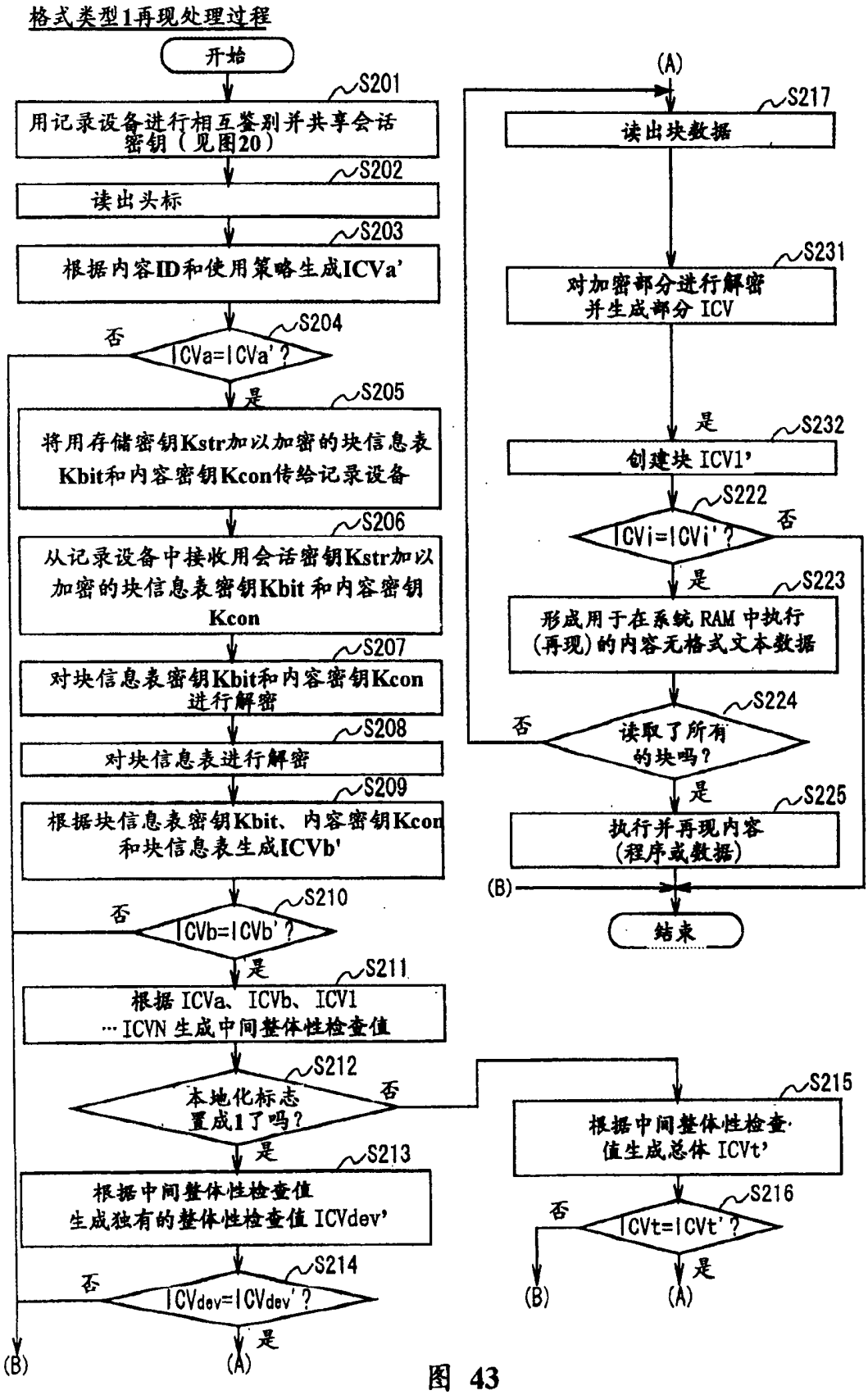

格式类型1再现处理过程
开始
S201
用记录设备进行相互鉴别并共享会话密钥（见图20）
S202
读出头标
S203
根据内容ID和使用策略生成ICVa'
S204
ICVa=ICVa'?
否
是
S205
将用存储密钥Kstr加以加密的块信息表Kbit和内容密钥Kcon传给记录设备
S206
从记录设备中接收用会话密钥Kstr加以加密的块信息表密钥Kbit和内容密钥Kcon
S207
对块信息表密钥Kbit和内容密钥Kcon进行解密
S208
对块信息表进行解密
S209
根据块信息表密钥Kbit、内容密钥Kcon和块信息表生成ICVb'
S210
ICVb=ICVb'?
否
是
S211
根据 ICVa、ICVb、ICV1 …ICVN 生成中间整体性检查值
S212
本地化标志置成1了吗?
否
是
S213
根据中间整体性检查值生成独有的整体性检查值 ICVdev'
S214
ICVdev=ICVdev'?
否
是
(B)
(A)
(A)
S217
读出块数据
S231
对加密部分进行解密并生成部分 ICV
是
S232
创建块 ICV1'
S222
ICVi=ICVi'?
否
是
S223
形成用于在系统 RAM 中执行(再现)的内容无格式文本数据
S224
读取了所有的块吗?
否
是
S225
执行并再现内容(程序或数据)
(B)
结束
S215
根据中间整体性检查值生成总体 ICVt'
S216
ICVt=ICVt'?
否
是
(B)
(A)

图 43

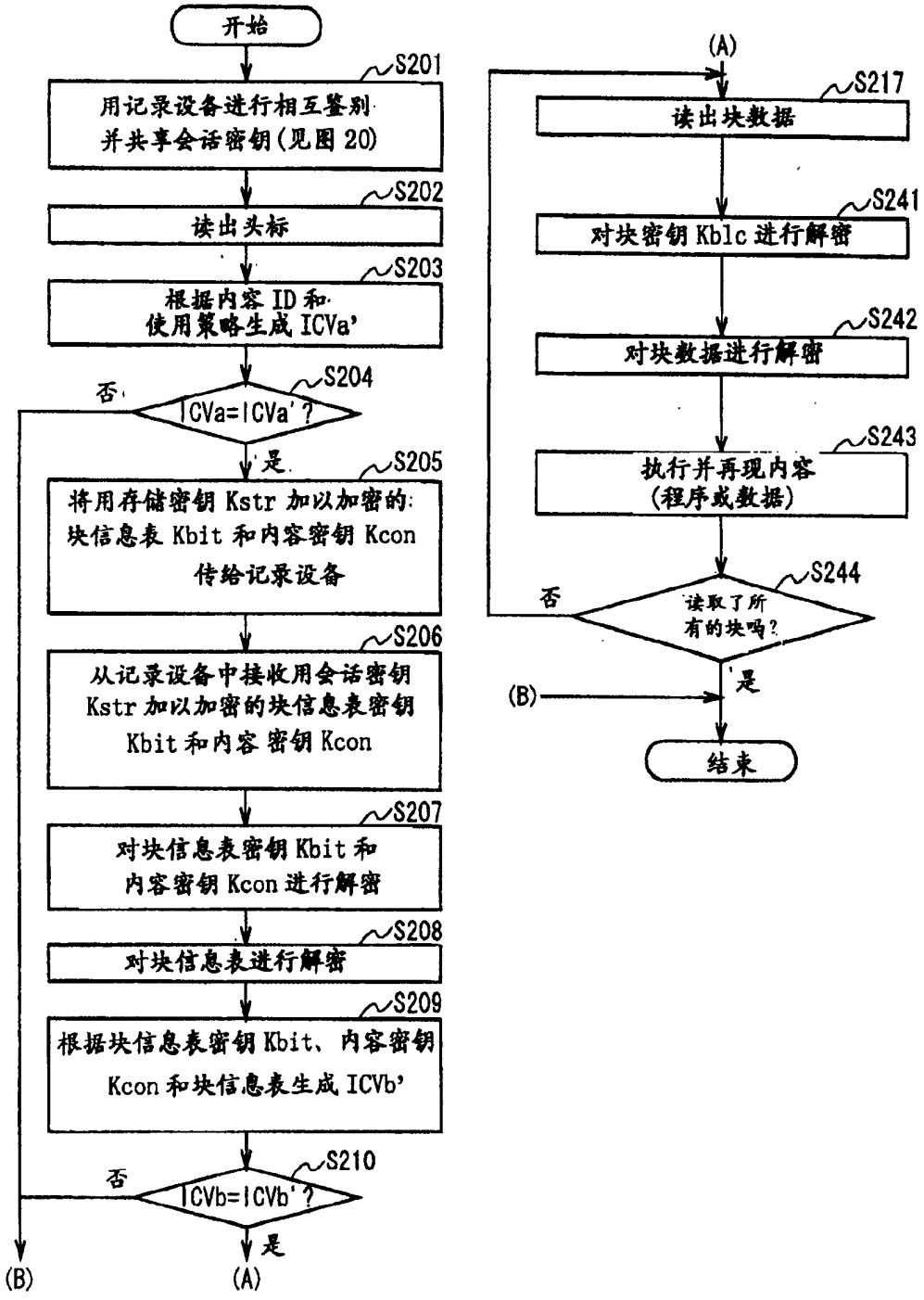

开始
S201
用记录设备进行相互鉴别
并共享会话密钥(见图 20)
S202
读出头标
S203
根据内容 ID 和
使用策略生成 ICVa'
S204
否
ICVa=ICVa'?
是
S205
将用存储密钥 Kstr 加以加密的
块信息表 Kbit 和内容密钥 Kcon
传给记录设备
S206
从记录设备中接收用会话密钥
Kstr 加以加密的块信息表密钥
Kbit 和内容 密钥 Kcon
S207
对块信息表密钥 Kbit 和
内容密钥 Kcon 进行解密
S208
对块信息表进行解密
S209
根据块信息表密钥 Kbit、内容密钥
Kcon 和块信息表生成 ICVb'
S210
否
ICVb=ICVb'?
是
(B)
(A)
(A)
S217
读出块数据
S241
对块密钥 Kblc 进行解密
S242
对块数据进行解密
S243
执行并再现内容
(程序或数据)
S244
否
读取了所
有的块吗?
是
(B)
结束

图 44

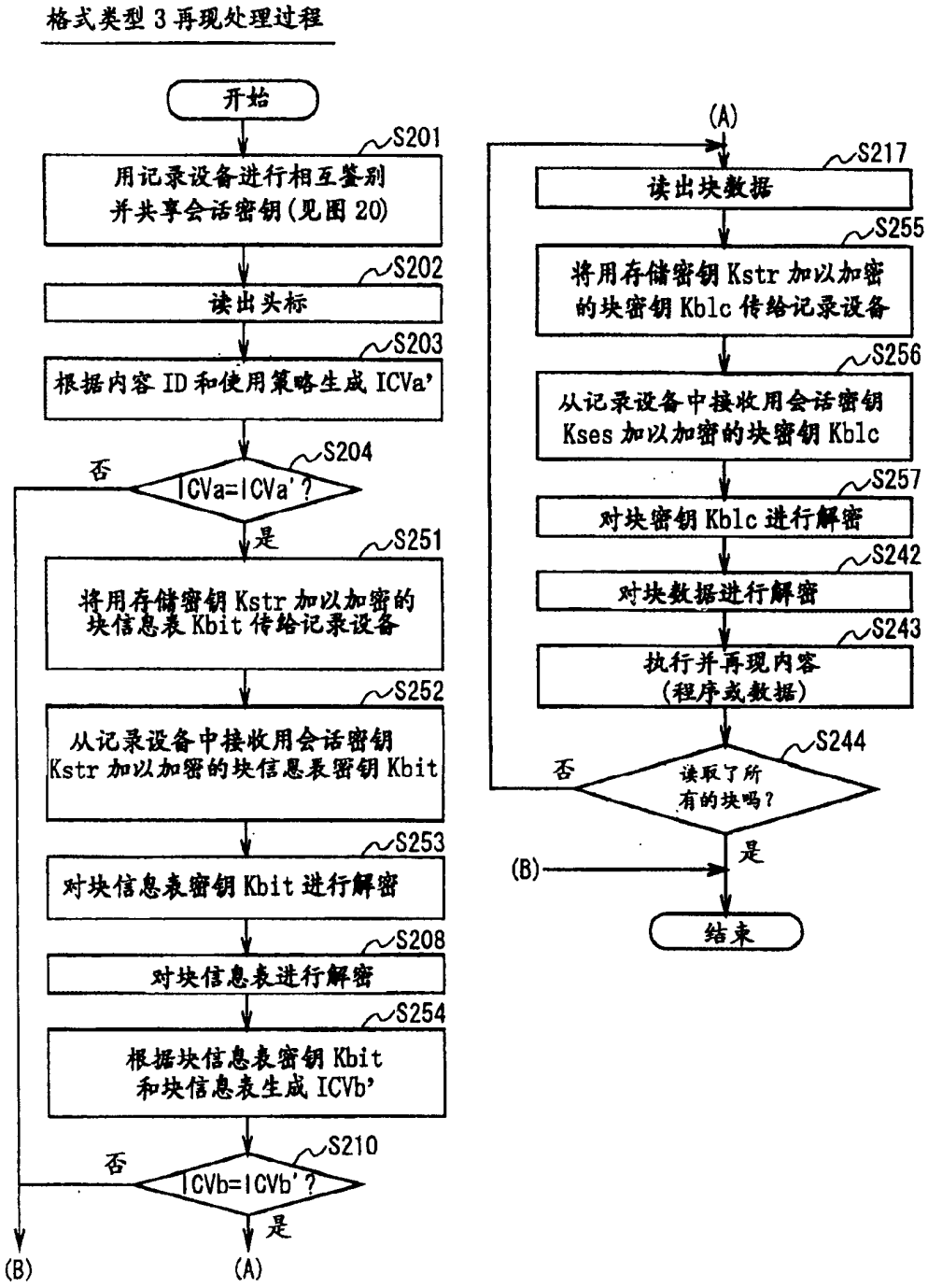

格式类型 3 再现处理过程
开始
S201
用记录设备进行相互鉴别
并共享会话密钥(见图 20)
S202
读出头标
S203
根据内容 ID 和使用策略生成 ICVa'
S204
否
ICVa=ICVa'?
是
S251
将用存储密钥 Kstr 加以加密的
块信息表 Kbit 传给记录设备
S252
从记录设备中接收用会话密钥
Kstr 加以加密的块信息表密钥 Kbit
S253
对块信息表密钥 Kbit 进行解密
S208
对块信息表进行解密
S254
根据块信息表密钥 Kbit
和块信息表生成 ICVb'
S210
否
ICVb=ICVb'?
是
(B)
(A)
(A)
S217
读出块数据
S255
将用存储密钥 Kstr 加以加密
的块密钥 Kblc 传给记录设备
S256
从记录设备中接收用会话密钥
Kses 加以加密的块密钥 Kblc
S257
对块密钥 Kblc 进行解密
S242
对块数据进行解密
S243
执行并再现内容
(程序或数据)
S244
否
读取了所
有的块吗?
是
(B)
结束

图 45

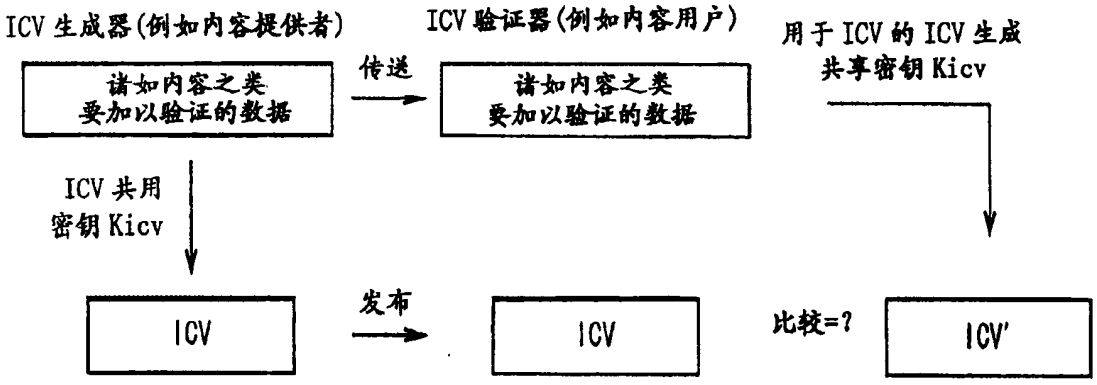

ICV 生成器(例如内容提供者)
ICV 验证器(例如内容用户)
用于 ICV 的 ICV 生成
共享密钥 Kicv
诸如内容之类
要加以验证的数据
传送
诸如内容之类
要加以验证的数据
ICV 共用
密钥 Kicv
ICV
发布
ICV
比较=?
ICV'

图 46

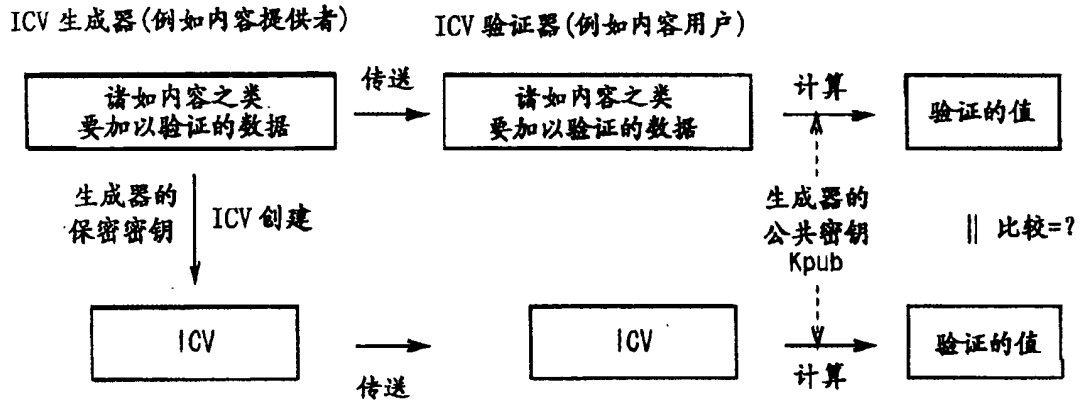

ICV 生成器(例如内容提供者)
ICV 验证器(例如内容用户)
诸如内容之类
要加以验证的数据
传送
诸如内容之类
要加以验证的数据
计算
验证的值
生成器的
保密密钥
ICV 创建
生成器的
公共密钥
Kpub
比较=?
ICV
传送
ICV
计算
验证的值

图 47

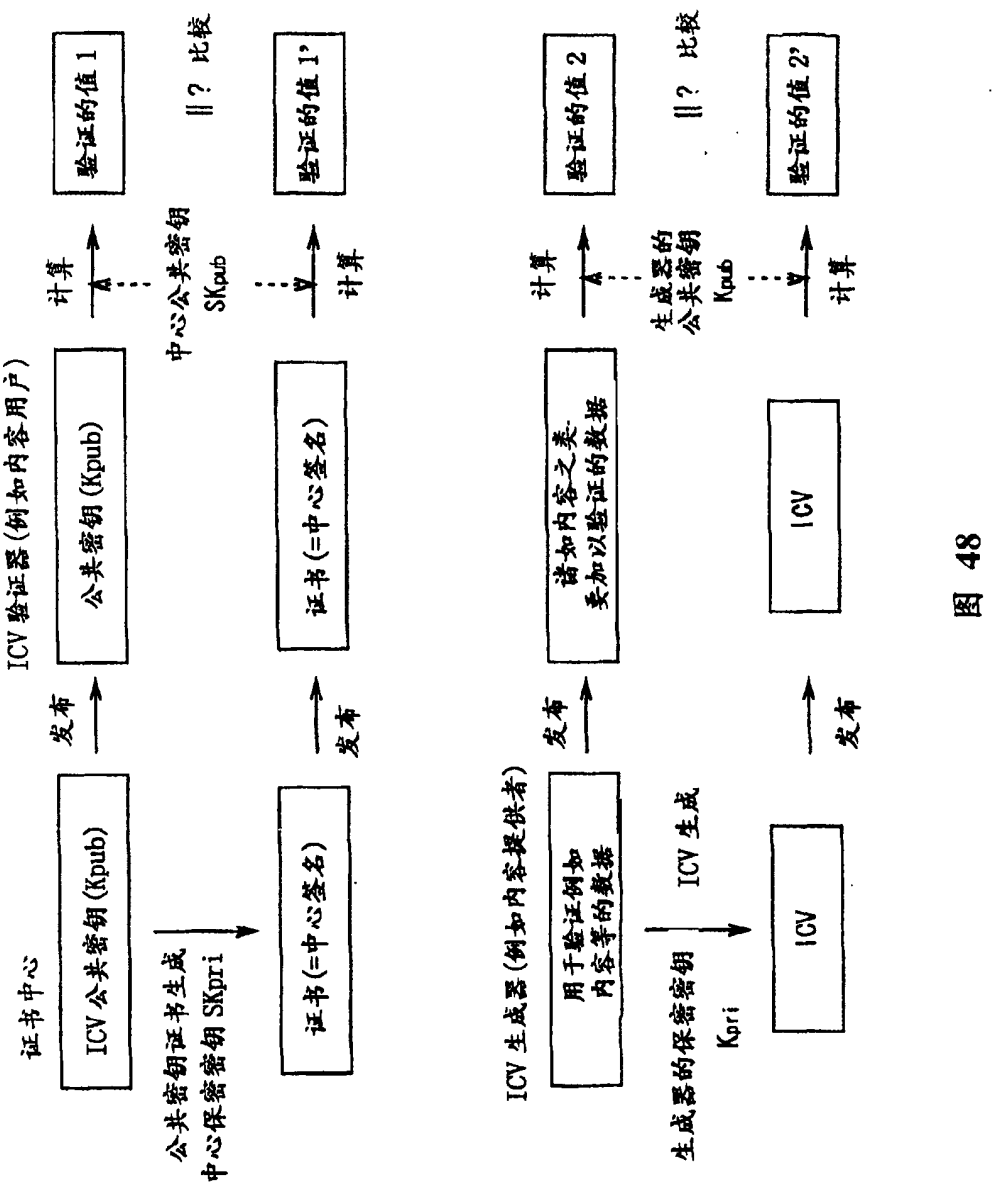

证书中心
ICV 公共密钥 (Kpub)
发布
ICV 验证器(例如内容用户)
公共密钥 (Kpub)
计算
验证的值 1
中心公共密钥
SKpub
=? 比较
公共密钥证书生成
中心保密密钥 SKpri
证书(=中心签名)
计算
证书(=中心签名)
发布
验证的值 1'
ICV 生成器(例如内容提供者)
用于验证例如
内容等的数据
发布
诸如内容之类
要加以验证的数据
计算
验证的值 2
生成器的公共密钥
Kpub
=? 比较
生成器的保密密钥
Kpri
ICV 生成
ICV
ICV
发布
计算
验证的值 2'

图 48

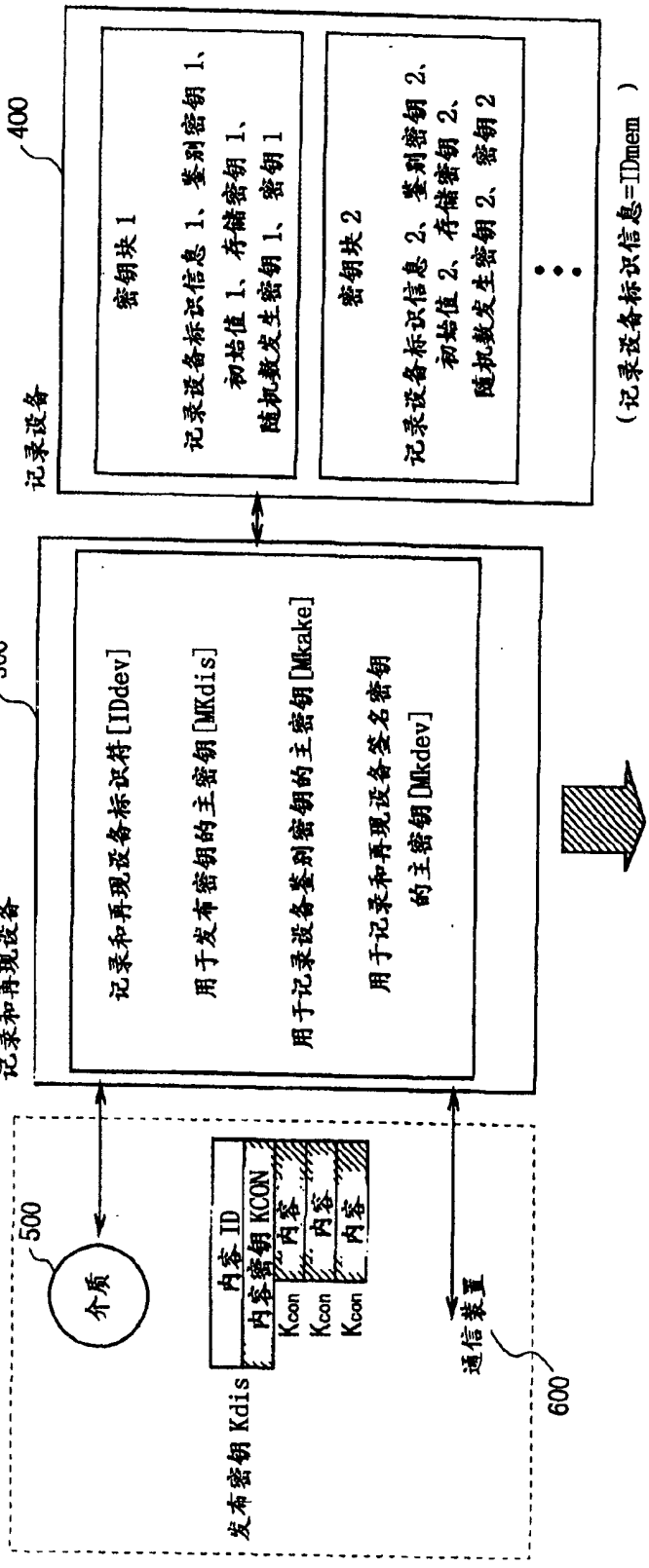

400
记录设备
密钥块 1
记录设备标识信息 1、鉴别密钥 1、
初始值 1、存储密钥 1、
随机数发生密钥 1、密钥 1
密钥块 2
记录设备标识信息 2、鉴别密钥 2、
初始值 2、存储密钥 2、
随机数发生密钥 2、密钥 2
(记录设备标识信息=IDmem)
300
记录和再现设备
记录和再现设备标识符[IDdev]
用于发布密钥的主密钥[MKdis]
用于记录设备鉴别密钥的主密钥[Mkake]
用于记录和再现设备签名密钥
的主密钥[Mkdev]
500
介质
内容 ID
内容密钥 KCON
Kcon
内容
Kcon
内容
Kcon
内容
发布密钥 Kdis
通信装置
600
发布密钥: KDIS=DES(MKdis, 内容 ID)
鉴别密钥: Kake=DES(MKake, IDmem)
记录和再现设备签名密钥: Kdev=DES(MKdev, IDdev)

图 49

用于根据主密钥生成各个密钥的方法-(1)

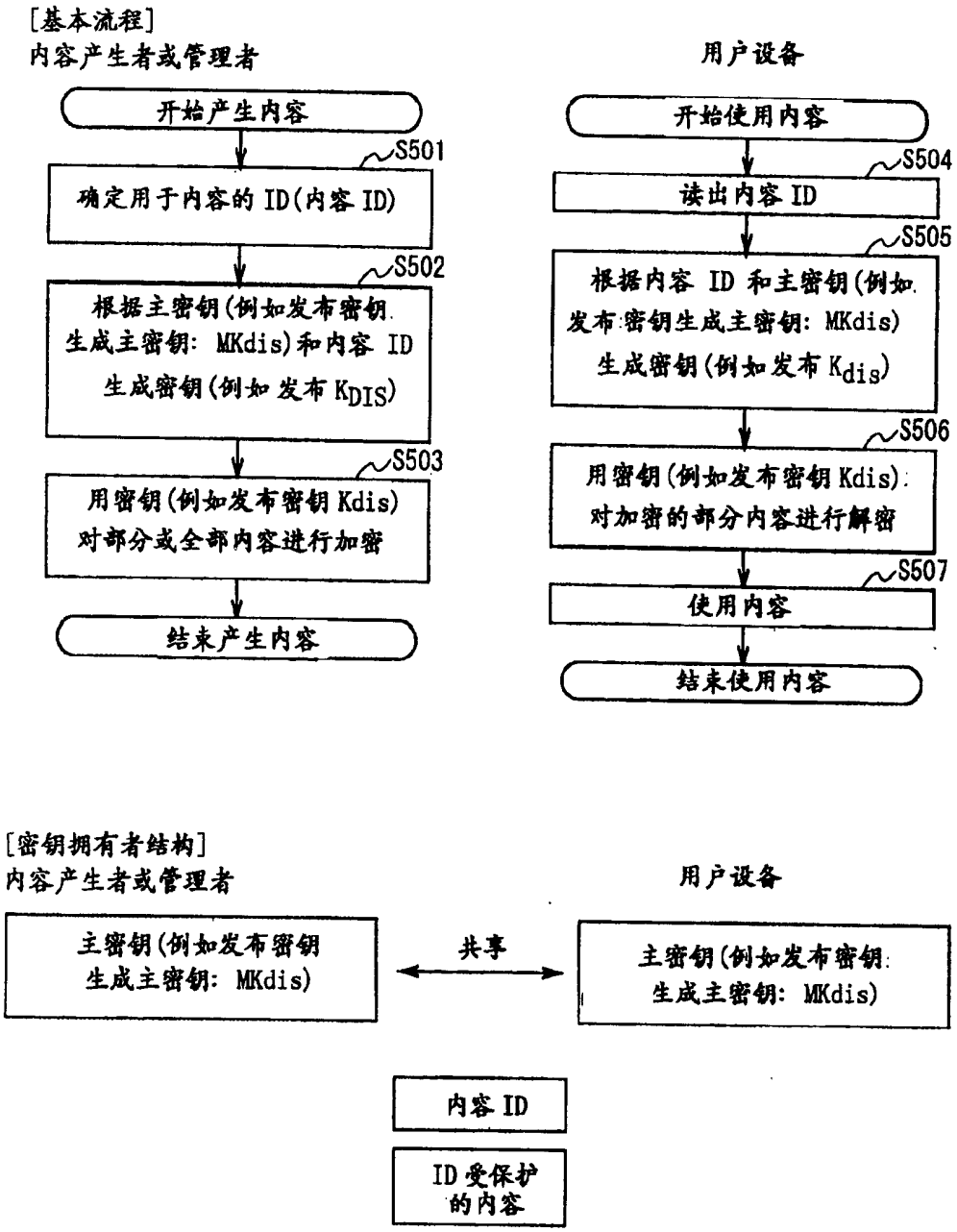
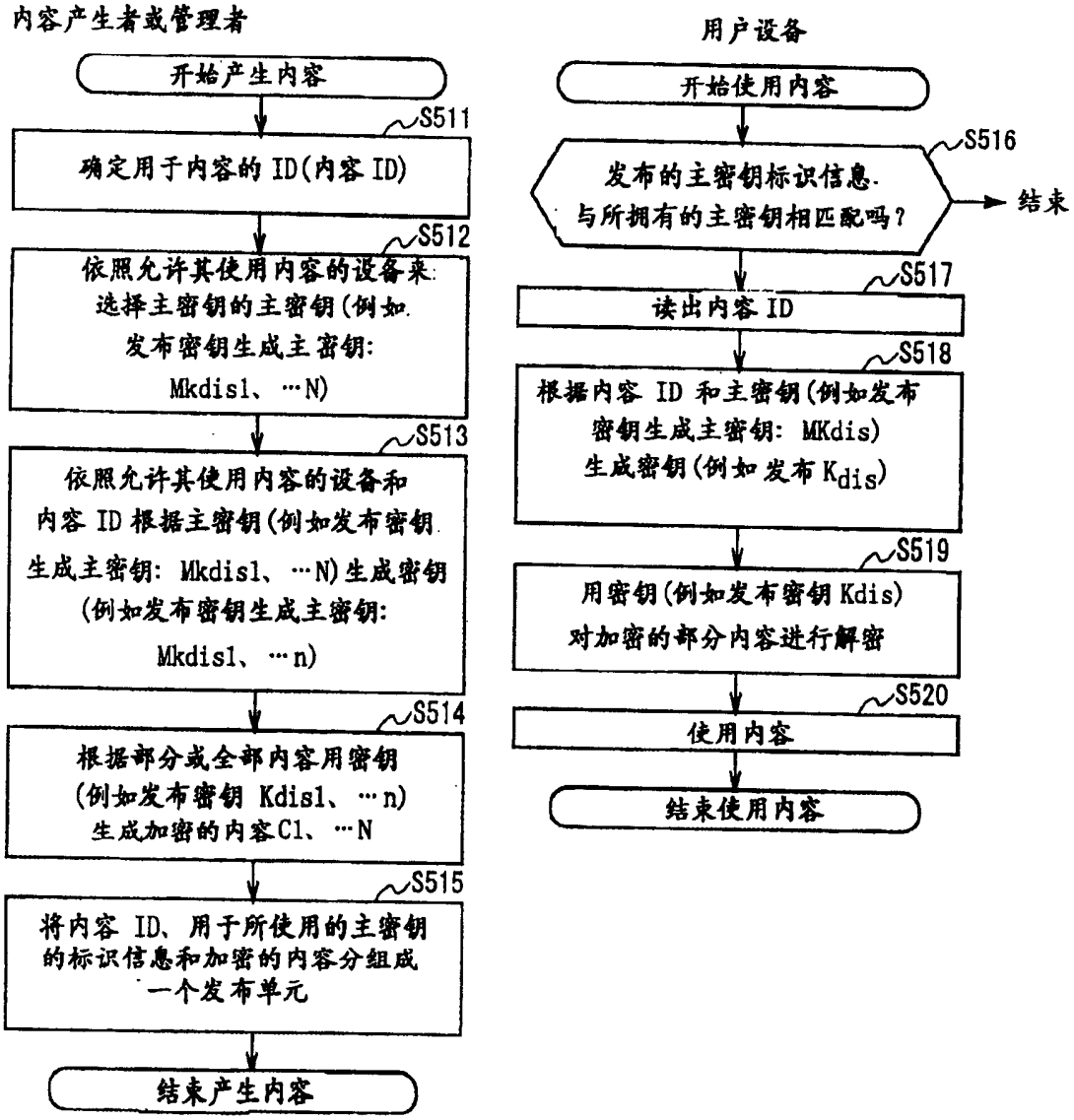


图 50

用于根据主密钥生成个别密钥的方法-(2)

[基本流程]



[密钥拥有者结构]

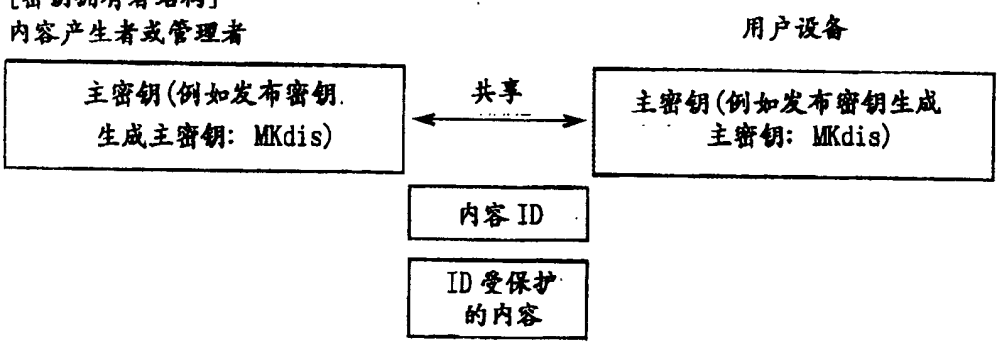


图 51

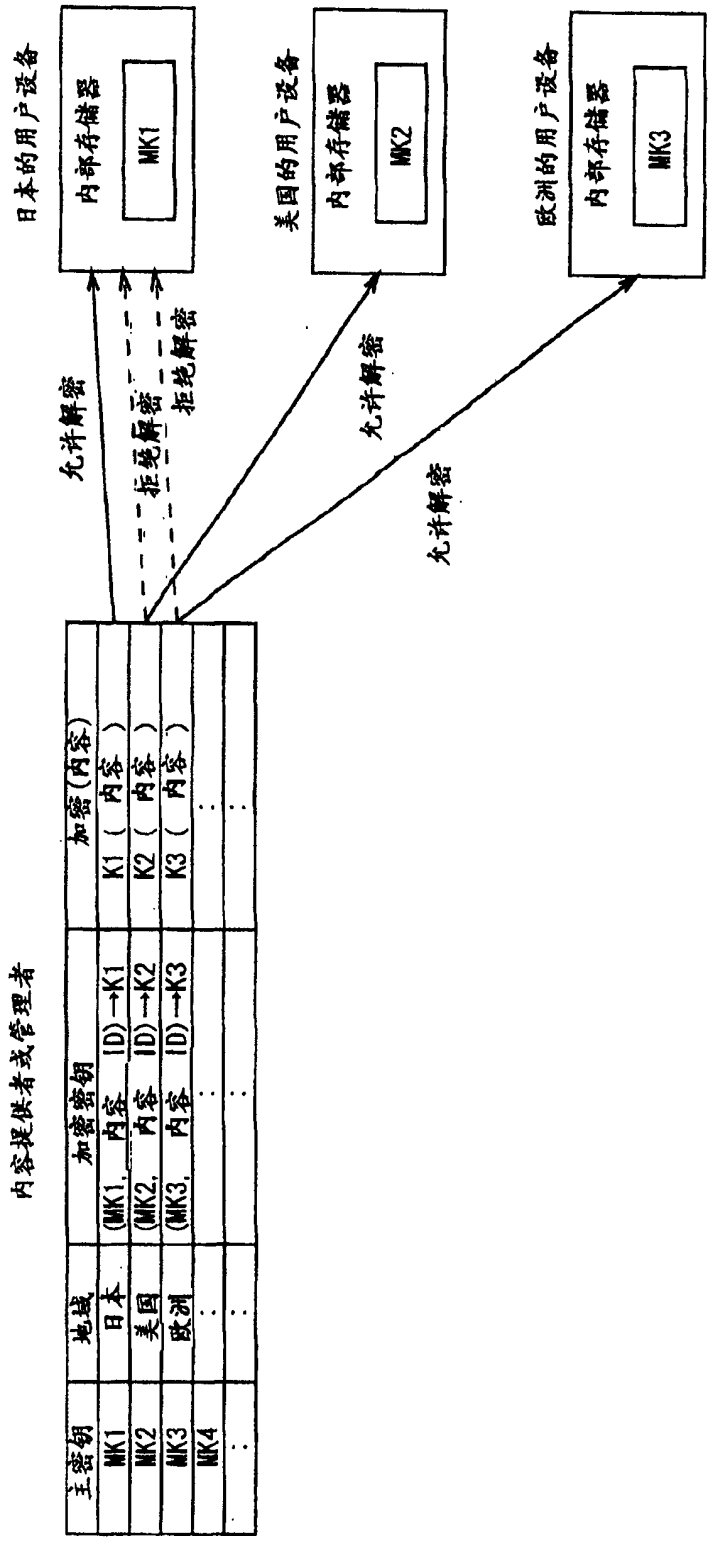
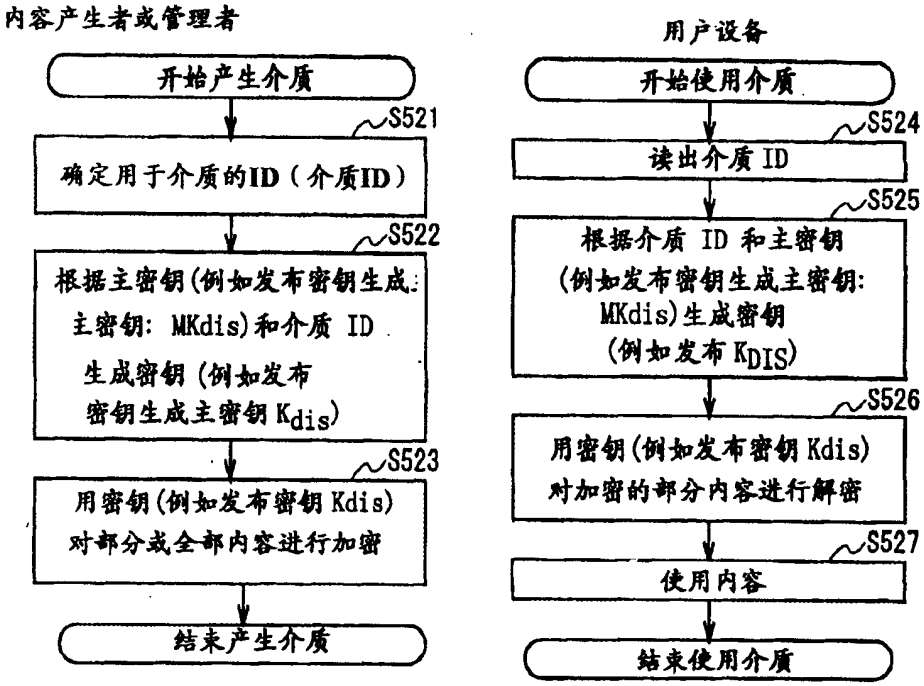

内容提供者或管理者
主密钥
地域
加密密钥
加密(内容)
MK1
日本
(MK1, 内容 ID)→K1
K1 (内容)
MK2
美国
(MK2, 内容 ID)→K2
K2 (内容)
MK3
欧洲
(MK3, 内容 ID)→K3
K3 (内容)
MK4
允许解密
拒绝解密
允许解密
允许解密
日本的用户设备
内部存储器
MK1
美国的用户设备
内部存储器
MK2
欧洲的用户设备
内部存储器
MK3

图 52

用于根据主密钥生成个别密钥的方法-（3）

[基本流程]



[密钥拥有者结构]

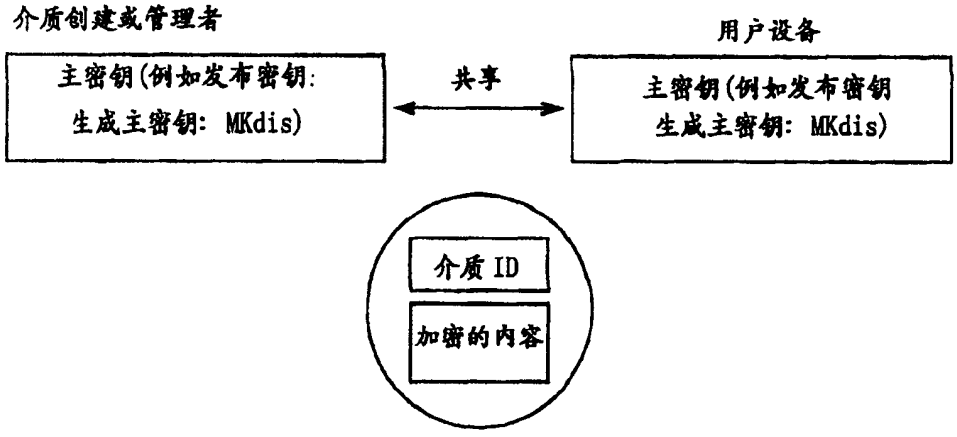
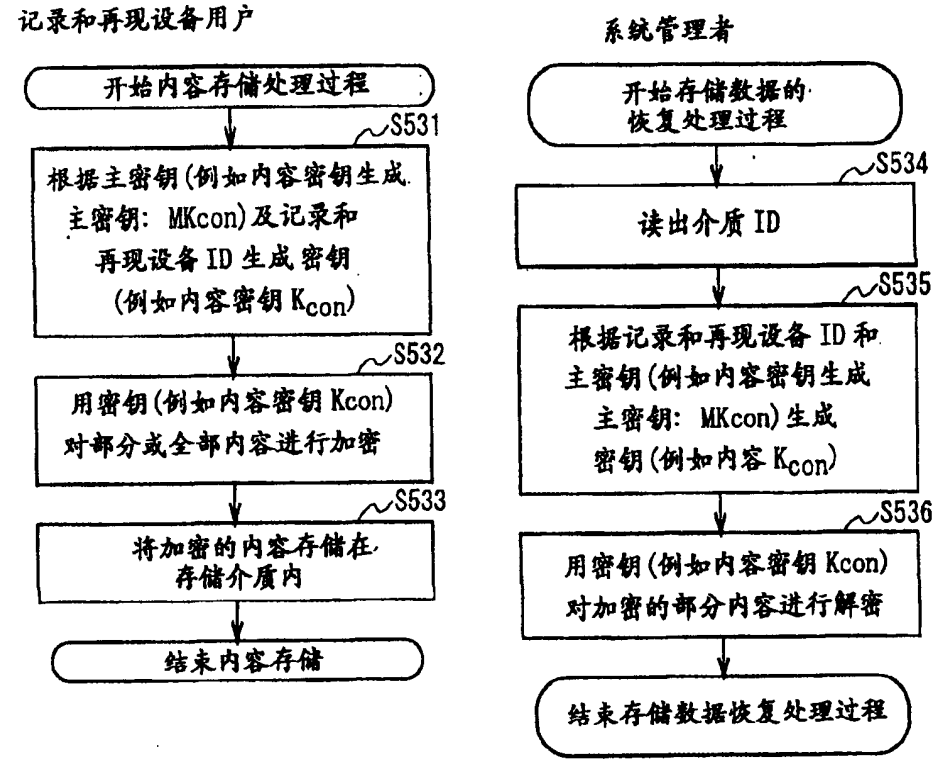


图 53

用于根据主密钥生成个别密钥的方法-(4)

[基本流程]



[密钥拥有者结构]

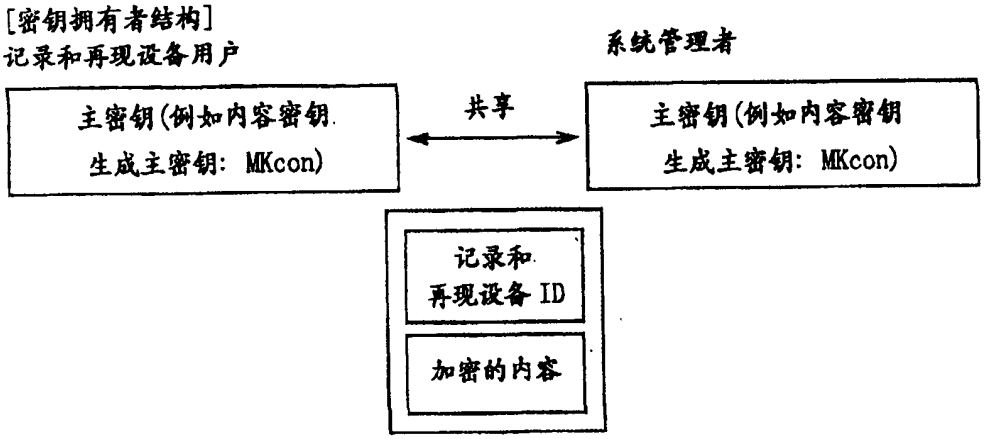
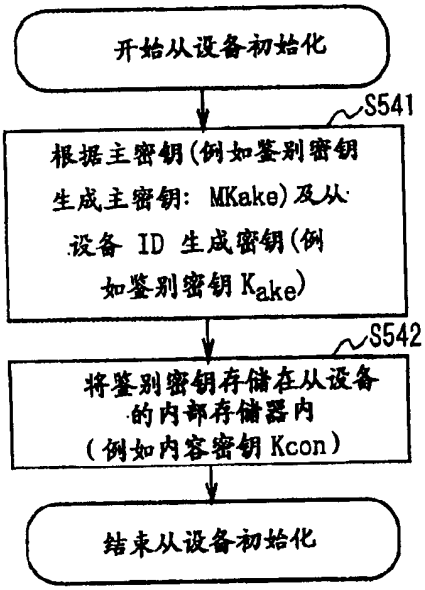


图 54

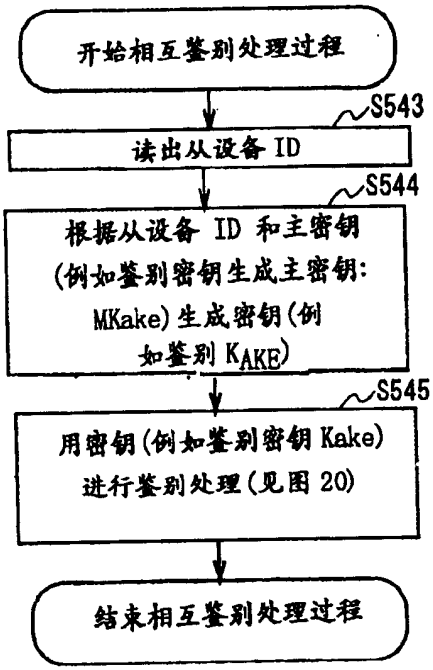
用于根据主密钥生成各个密钥的方法-(5)

[基本流程]

从设备(例如记录设备)



主设备(例如记录和再现设备)



[密钥拥有者结构]

从设备(例如记录设备)

主设备(例如记录和再现设备)

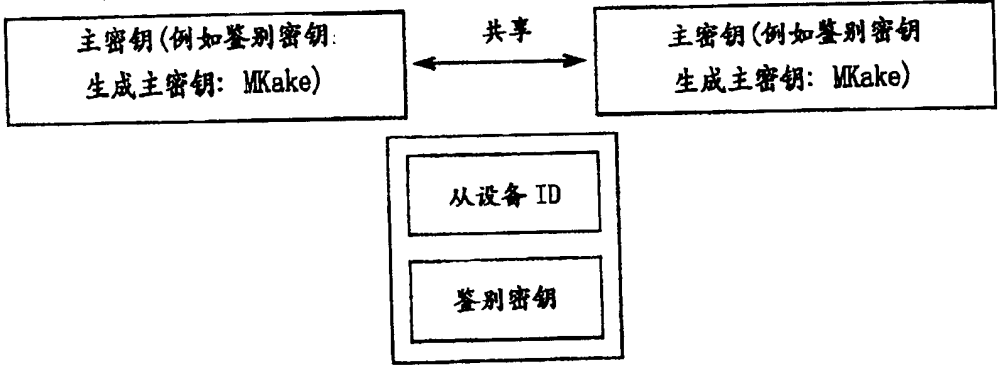


图 55

用于根据主密钥生成个别密钥的方法-(5)

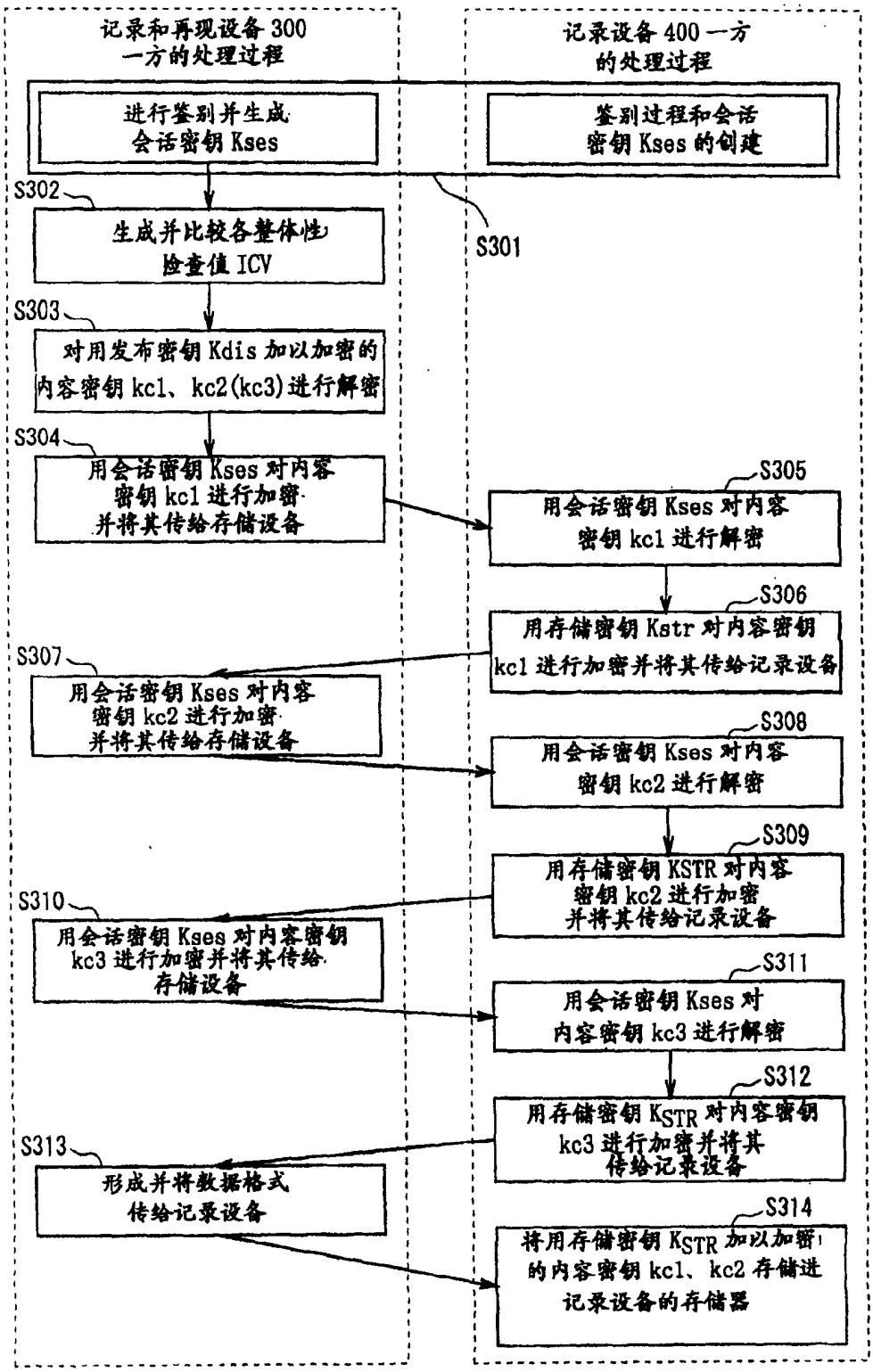


图 56

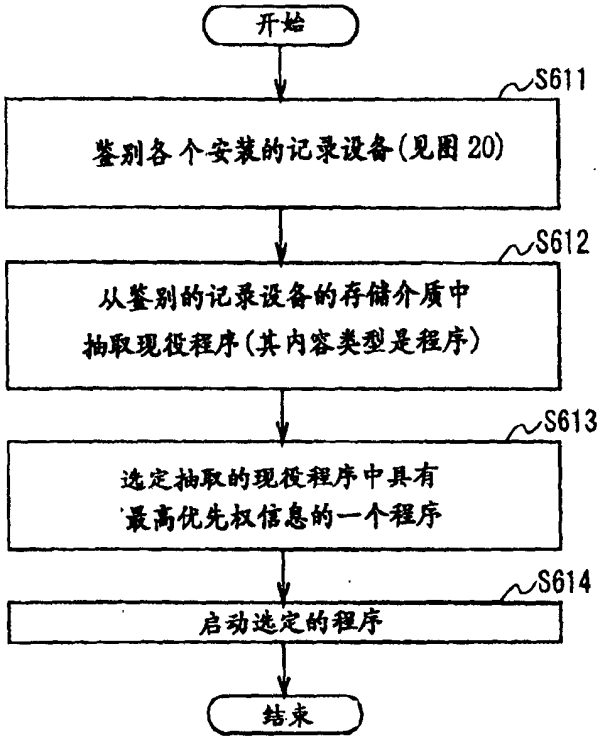

开始
S611
鉴别各个安装的记录设备(见图20)
S612
从鉴别的记录设备的存储介质中
抽取现役程序(其内容类型是程序)
S613
选定抽取的现役程序中具有
最高优先权信息的一个程序
S614
启动选定的程序
结束

图 57

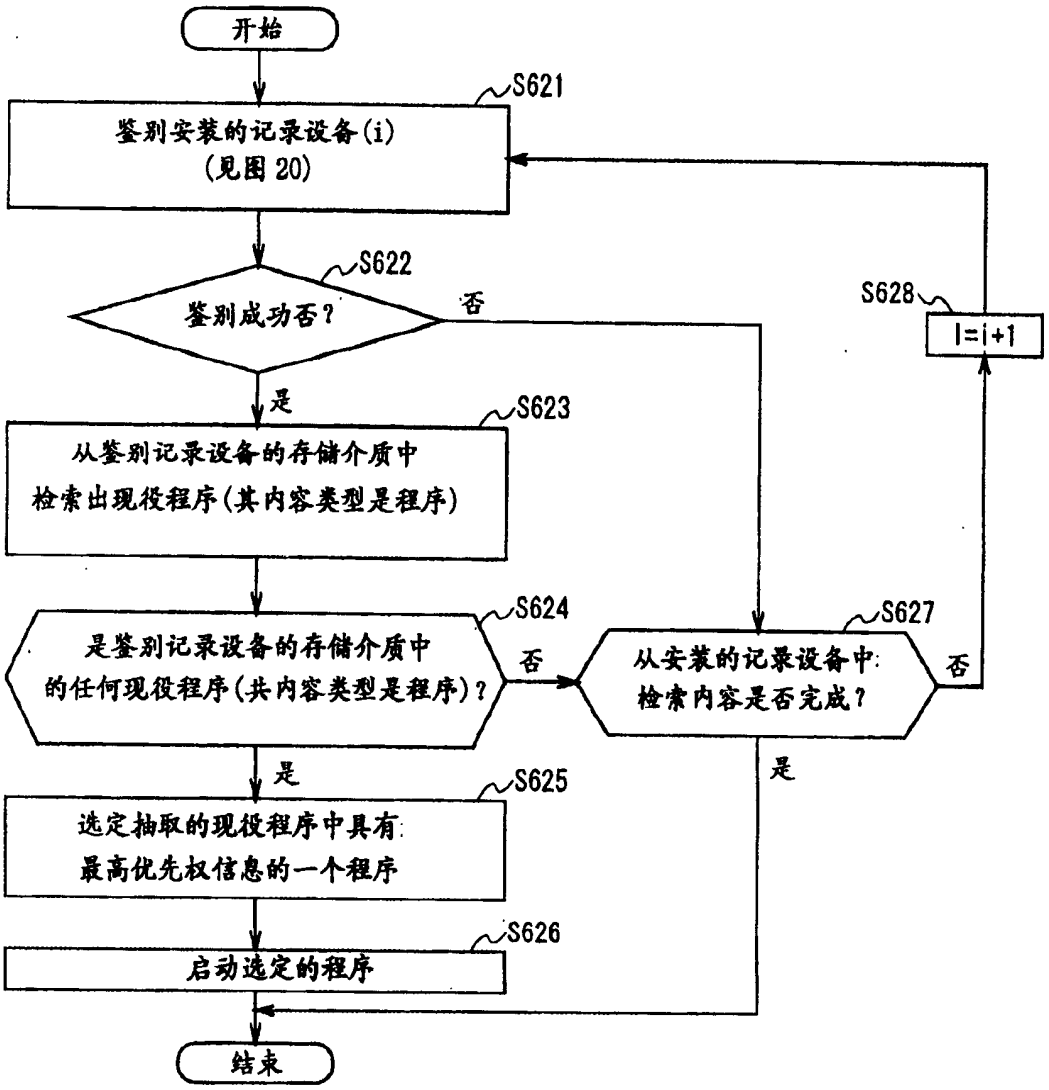

开始
S621
鉴别安装的记录设备(i)
(见图 20)
S622
鉴别成功否?
否
是
S628
I=I+1
S623
从鉴别记录设备的存储介质中
检索出现役程序(其内容类型是程序)
S624
是鉴别记录设备的存储介质中
的任何现役程序(其内容类型是程序)?
否
S627
从安装的记录设备中
检索内容是否完成?
否
是
是
S625
选定抽取的现役程序中具有
最高优先权信息的一个程序
S626
启动选定的程序
结束

图 58

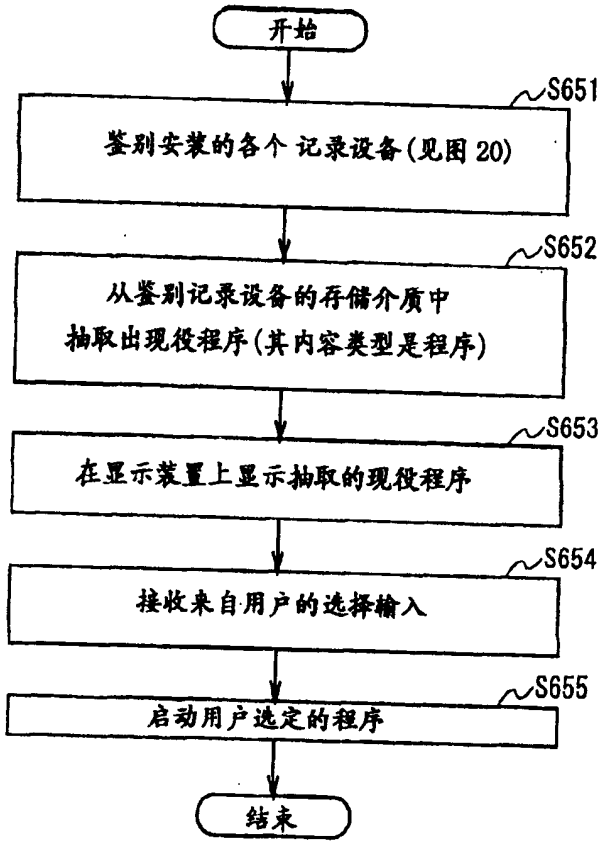

开始
S651
鉴别安装的各个记录设备(见图20)
S652
从鉴别记录设备的存储介质中
抽取出现役程序(其内容类型是程序)
S653
在显示装置上显示抽取的现役程序
S654
接收来自用户的选择输入
S655
启动用户选定的程序
结束

图 59

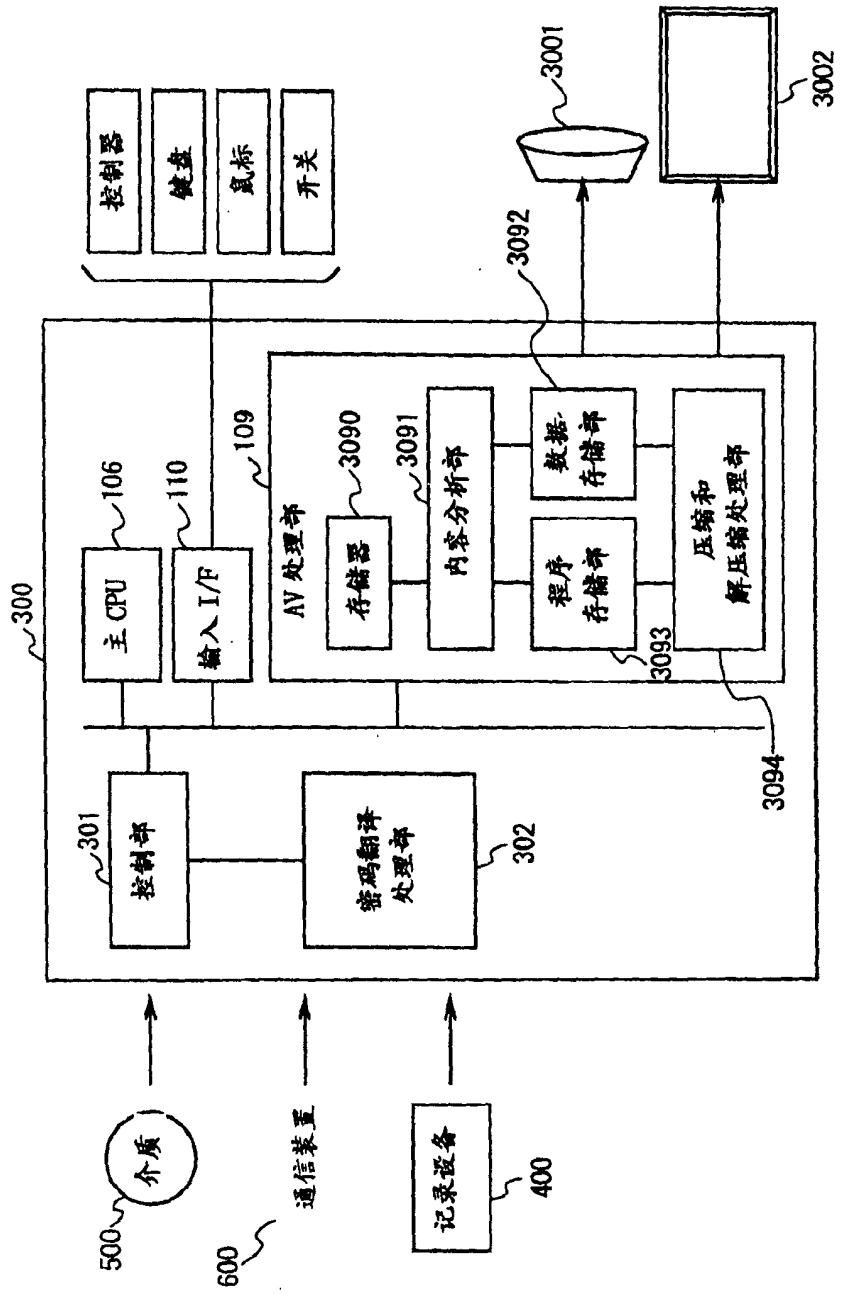

控制器
键盘
鼠标
开关
3001
3002
3092
300
106
110
109
3090
3091
主 CPU
输入 I/F
AV 处理部
存储器
内容分析部
数据
存储部
程序
存储部
压缩和
解压缩处理部
3093
3094
301
控制部
密码翻译
处理部
302
介质
500
通信装置
600
记录设备
400

图 60

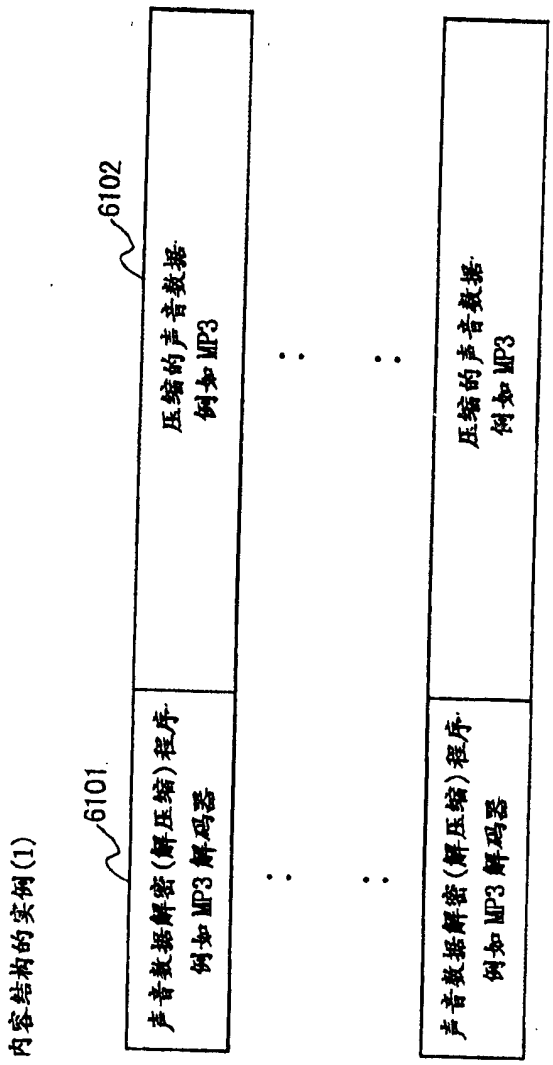

内容结构的实例(1)
6101
声音数据解密(解压缩)程序
例如 MP3 解码器
6102
压缩的声音数据
例如 MP3
声音数据解密(解压缩)程序
例如 MP3 解码器
压缩的声音数据
例如 MP3

图 61

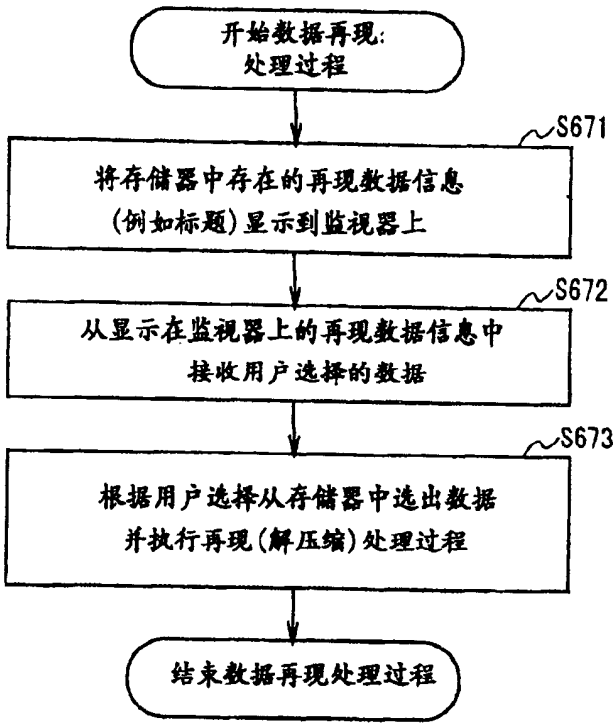

开始数据再现:
处理过程
S671
将存储器中存在的再现数据信息
(例如标题)显示到监视器上
S672
从显示在监视器上的再现数据信息中
接收用户选择的数据
S673
根据用户选择从存储器中选出数据
并执行再现(解压缩)处理过程
结束数据再现处理过程

图 62

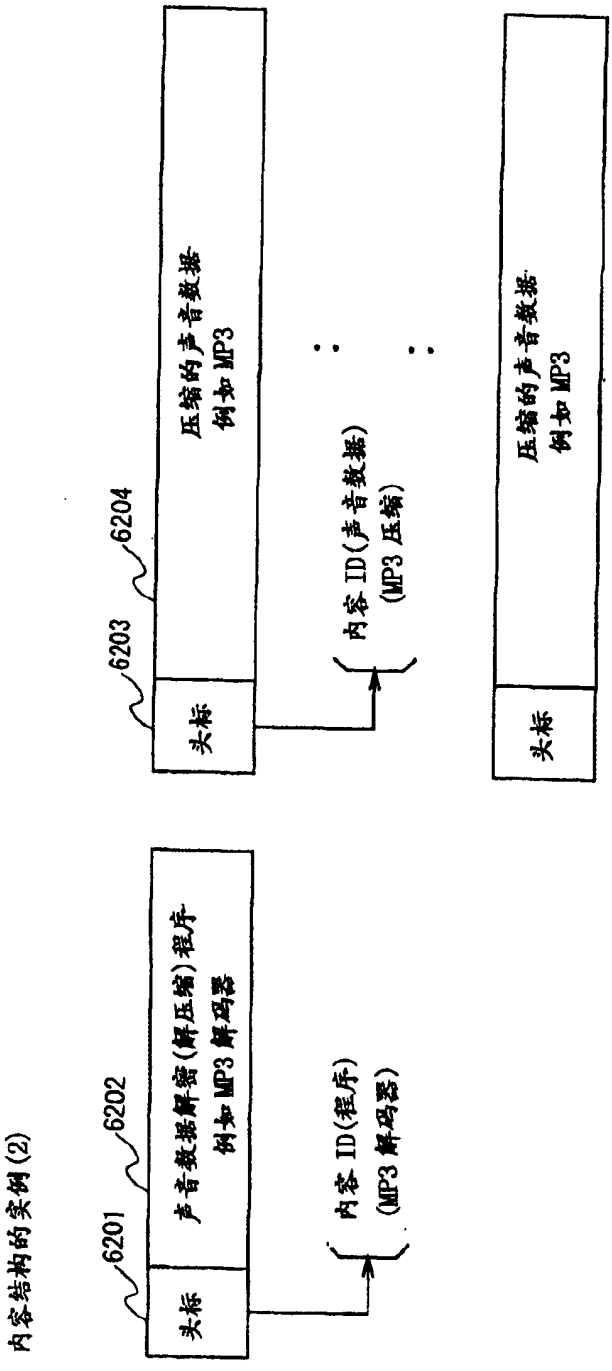

内容结构的实例(2)
6201
头标
6202
声音数据解密(解压缩)程序
例如 MP3 解码器
内容 ID(程序)
(MP3 解码器)
6203
头标
6204
压缩的声音数据
例如 MP3
内容 ID(声音数据)
(MP3 压缩)
头标
压缩的声音数据
例如 MP3

图 63

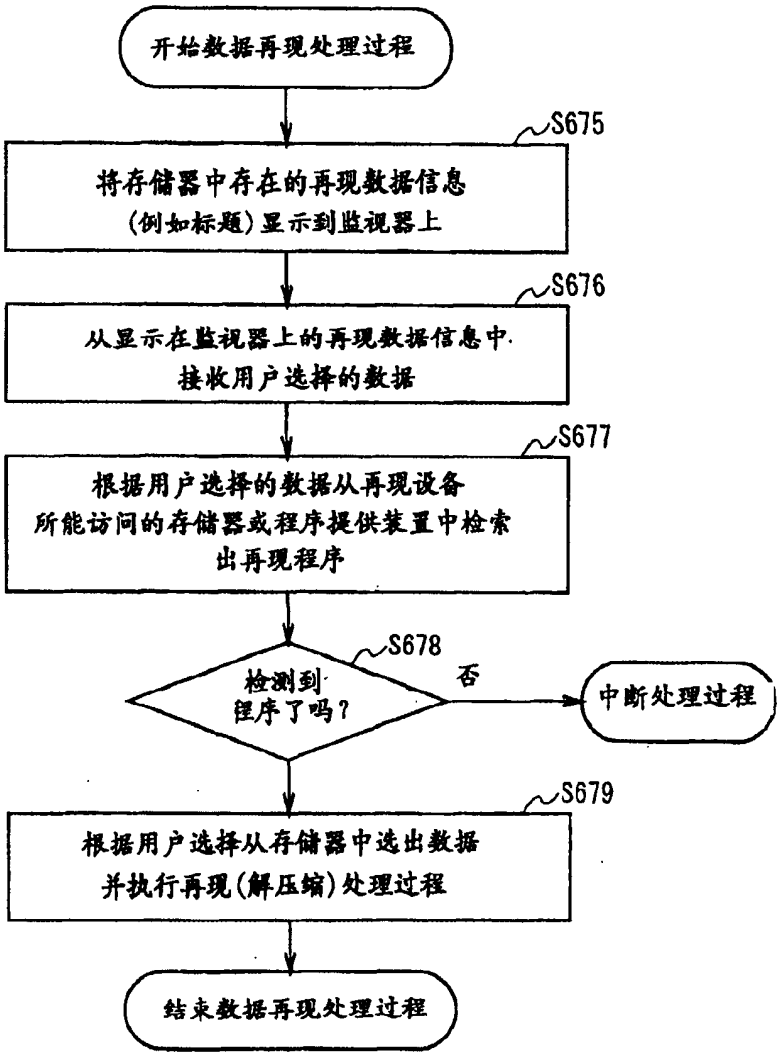

开始数据再现处理过程
S675
将存储器中存在的再现数据信息
(例如标题)显示到监视器上
S676
从显示在监视器上的再现数据信息中
接收用户选择的数据
S677
根据用户选择的数据从再现设备
所能访问的存储器或程序提供装置中检索
出再现程序
S678
检测到
程序了吗?
否
中断处理过程
S679
根据用户选择从存储器中选出数据
并执行再现(解压缩)处理过程
结束数据再现处理过程

图 64

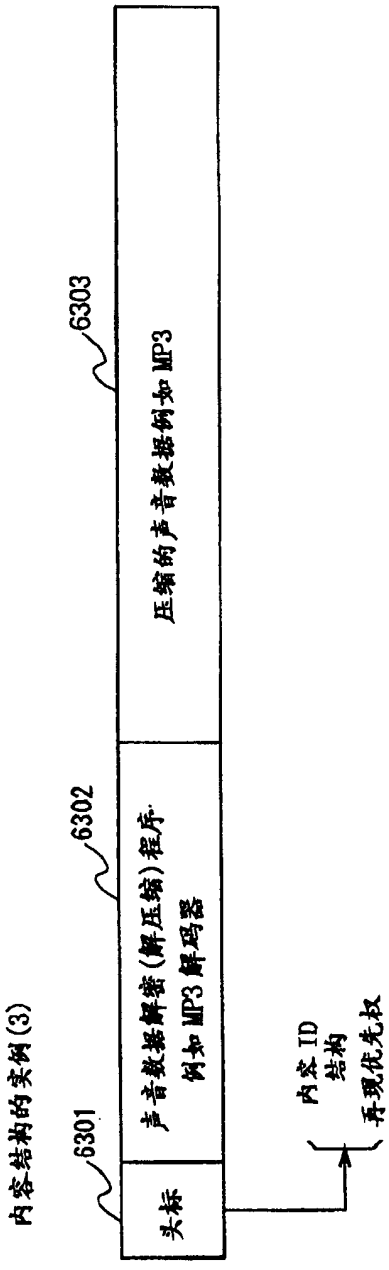

内容结构的实例(3)
6301
头标
6302
声音数据解密(解压缩)程序·
例如 MP3 解码器
6303
压缩的声音数据例如 MP3
内容 ID
结构
再现优先权

图 65

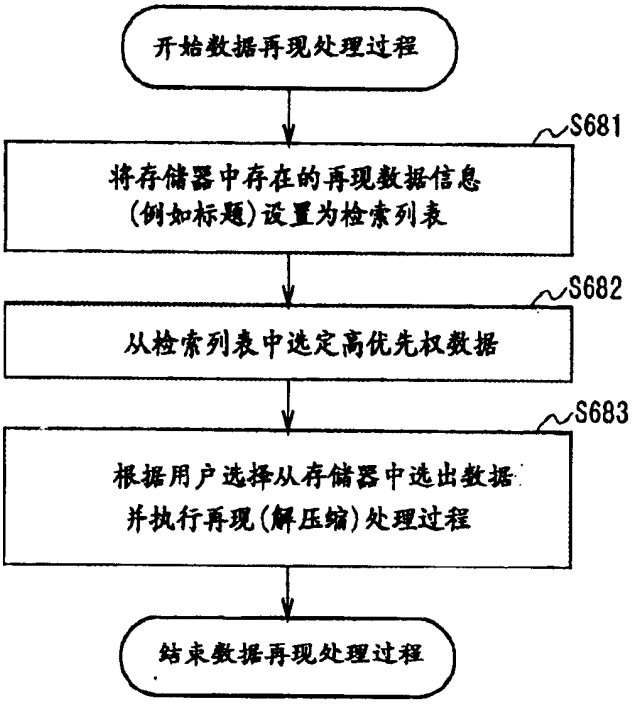

开始数据再现处理过程
S681
将存储器中存在的再现数据信息
(例如标题)设置为检索列表
S682
从检索列表中选定高优先权数据
S683
根据用户选择从存储器中选出数据
并执行再现(解压缩)处理过程
结束数据再现处理过程

图 66

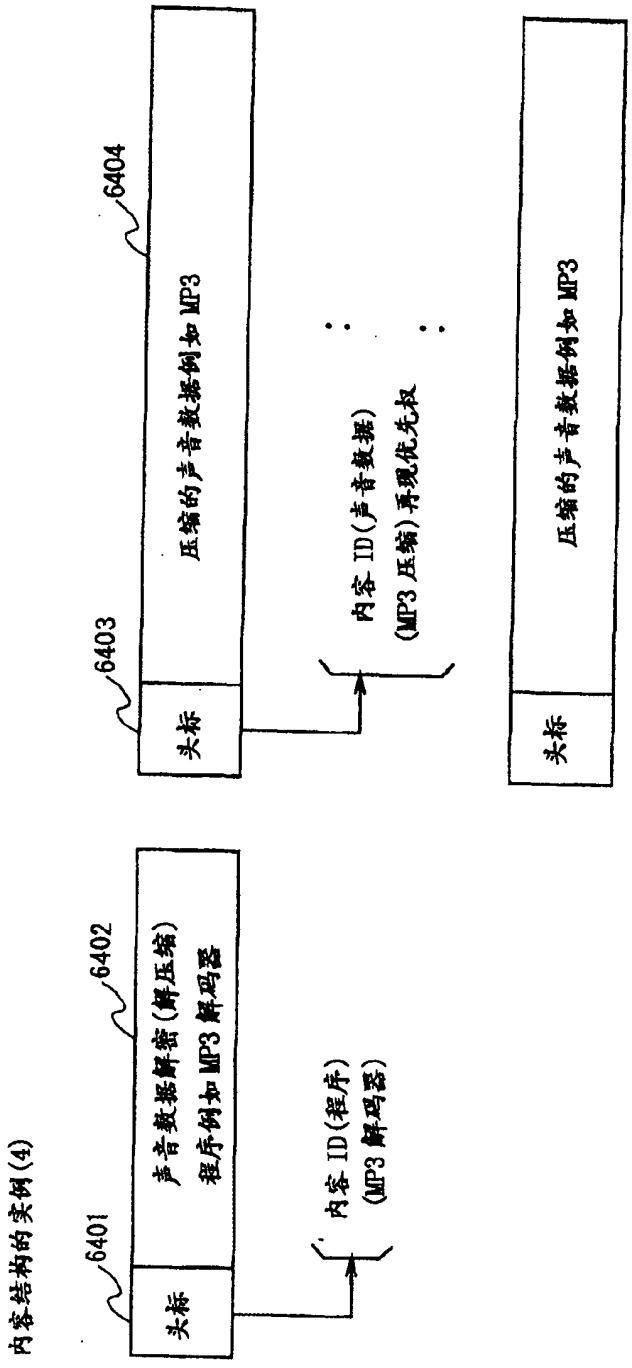

内容结构的实例(4)
6401
头标
6402
声音数据解密(解压缩)
程序例如 MP3 解码器
内容 ID(程序)
(MP3 解码器)
6403
头标
6404
压缩的声音数据例如 MP3
内容 ID(声音数据)
(MP3 压缩)再现优先权
头标
压缩的声音数据例如 MP3

图 67

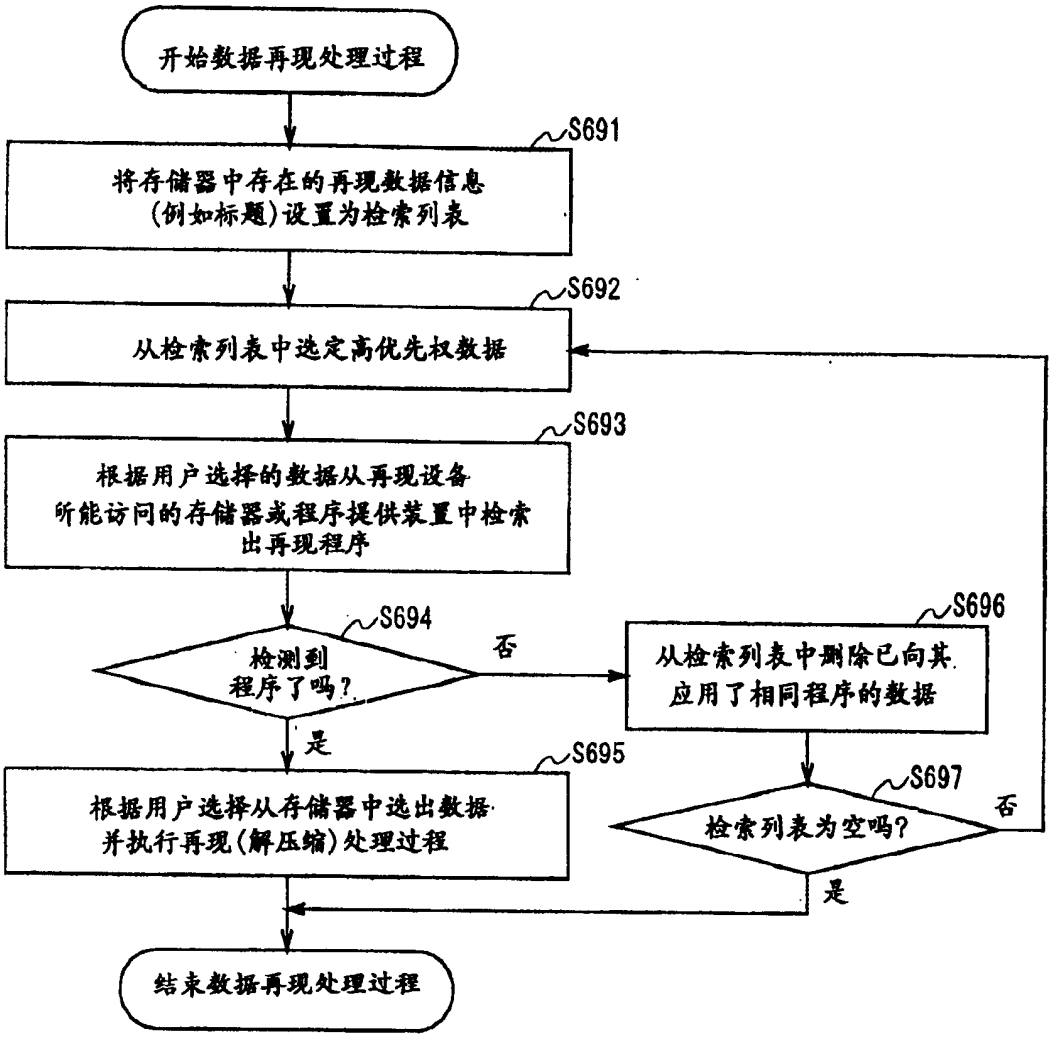

开始数据再现处理过程
S691
将存储器中存在的再现数据信息(例如标题)设置为检索列表
S692
从检索列表中选定高优先权数据
S693
根据用户选择的数据从再现设备所能访问的存储器或程序提供装置中检索出再现程序
S694
检测到程序了吗?
否
是
S695
根据用户选择从存储器中选出数据并执行再现(解压缩)处理过程
S696
从检索列表中删除已向其应用了相同程序的数据
S697
检索列表为空吗?
否
是
结束数据再现处理过程

图 68

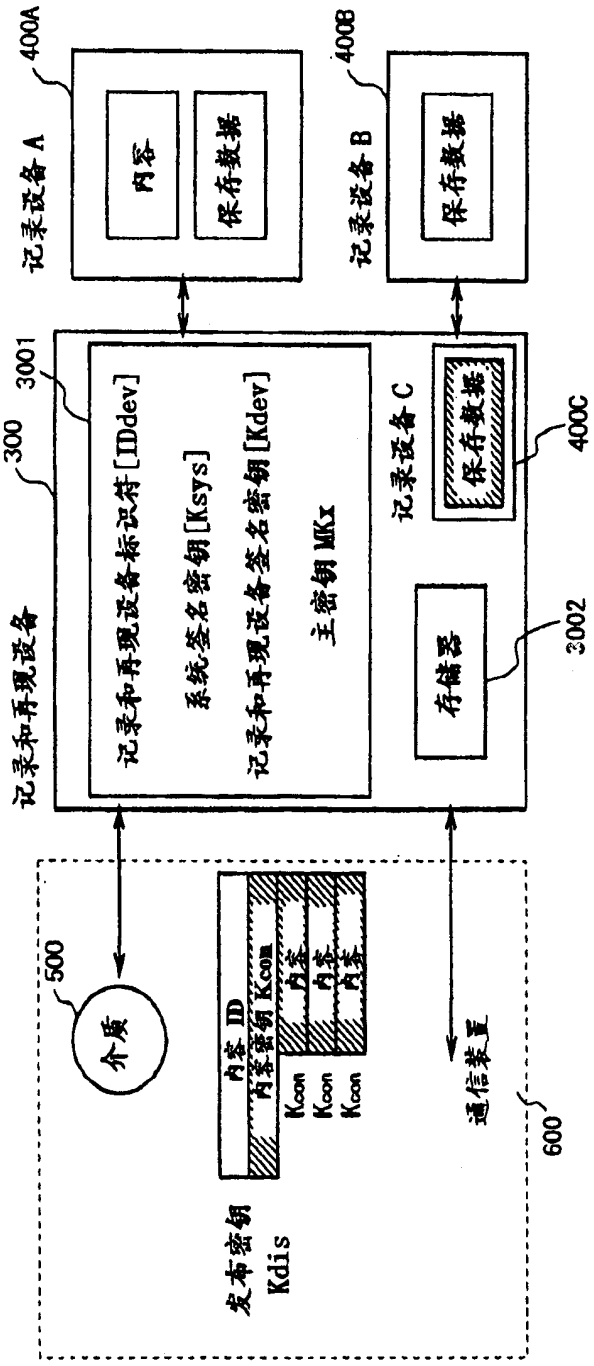

400A
记录设备 A
内容
保存数据
400B
记录设备 B
保存数据
3001
300
记录和再现设备
记录和再现设备标识符[IDdev]
系统签名密钥[Ksys]
记录和再现设备签名密钥[Kdev]
主密钥 MKx
记录设备 C
保存数据
400C
存储器
3002
500
介质
内容 ID
内容密钥 Kcon
内容
Kcon
内容
Kcon
内容
发布密钥
Kdis
通信装置
600

图 69

（1） 用内容独有密钥内容或系统共用密钥的保存数据存储处理过程的实例

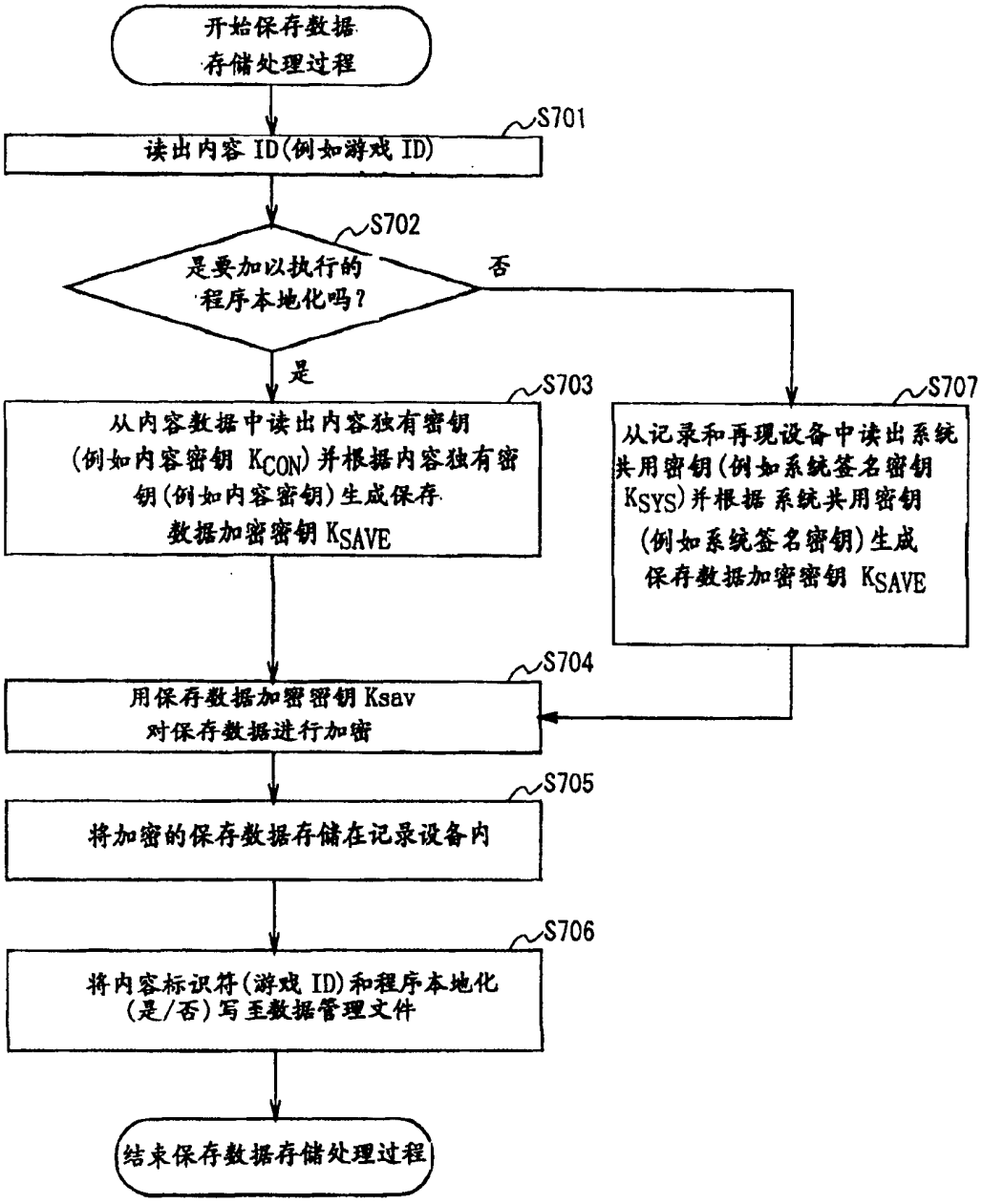


图 70

数据管理文件(1)

数据号	内容 ID(游戏 ID)	记录和再现设备 ID(IDDEV)	程序本地化
1	12345678...	56789012...	是
2	ABCDEF12...	09876543...	是
3	12245678...	58834762...	否
:	:	:	:

图 71

（2）用内容独有密钥或系统共用密钥的保存数据再现处理过程的实例

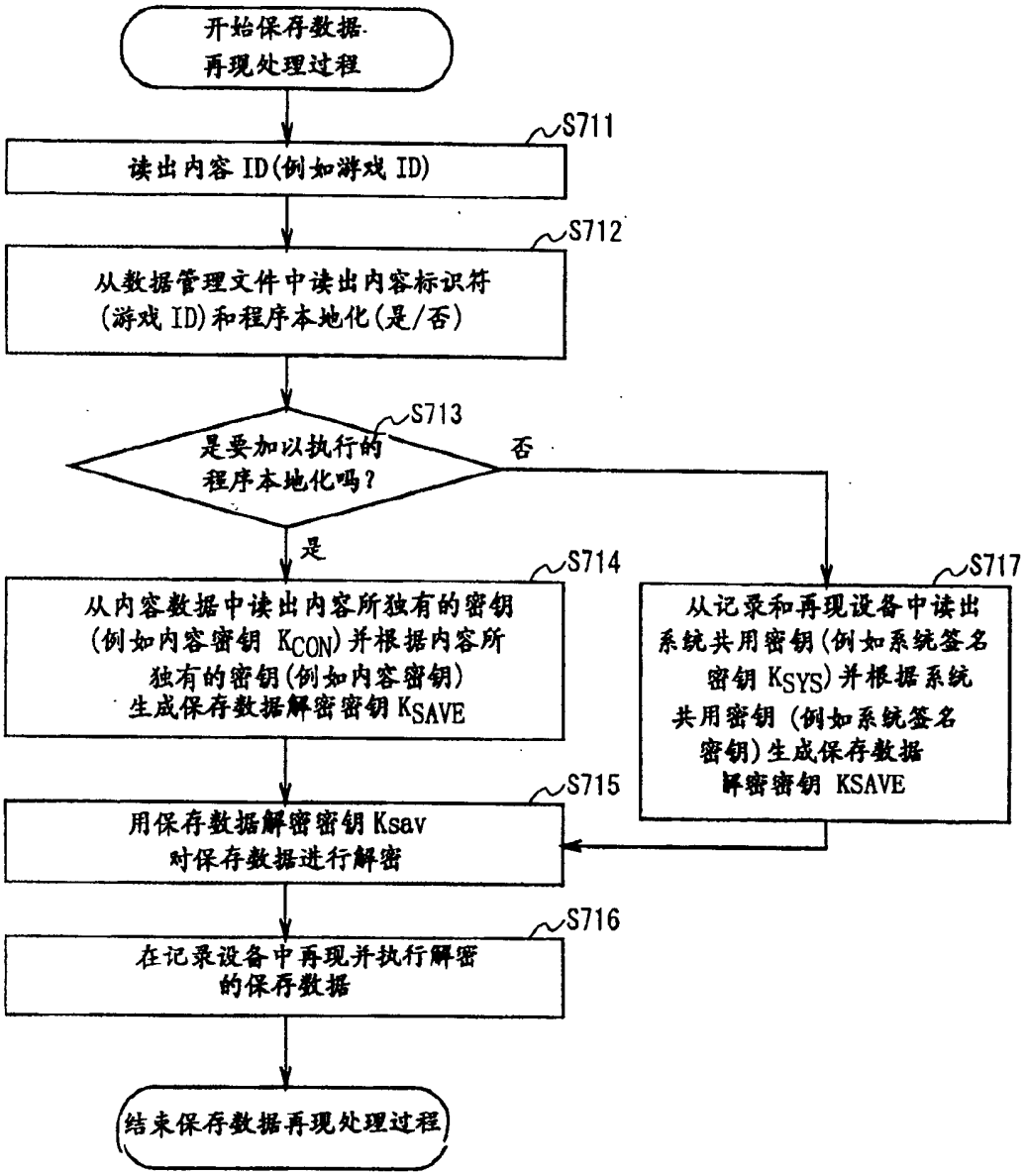


图 72

（3）用内容 ID 或系统共用密钥的保存数据存储处理过程的实例

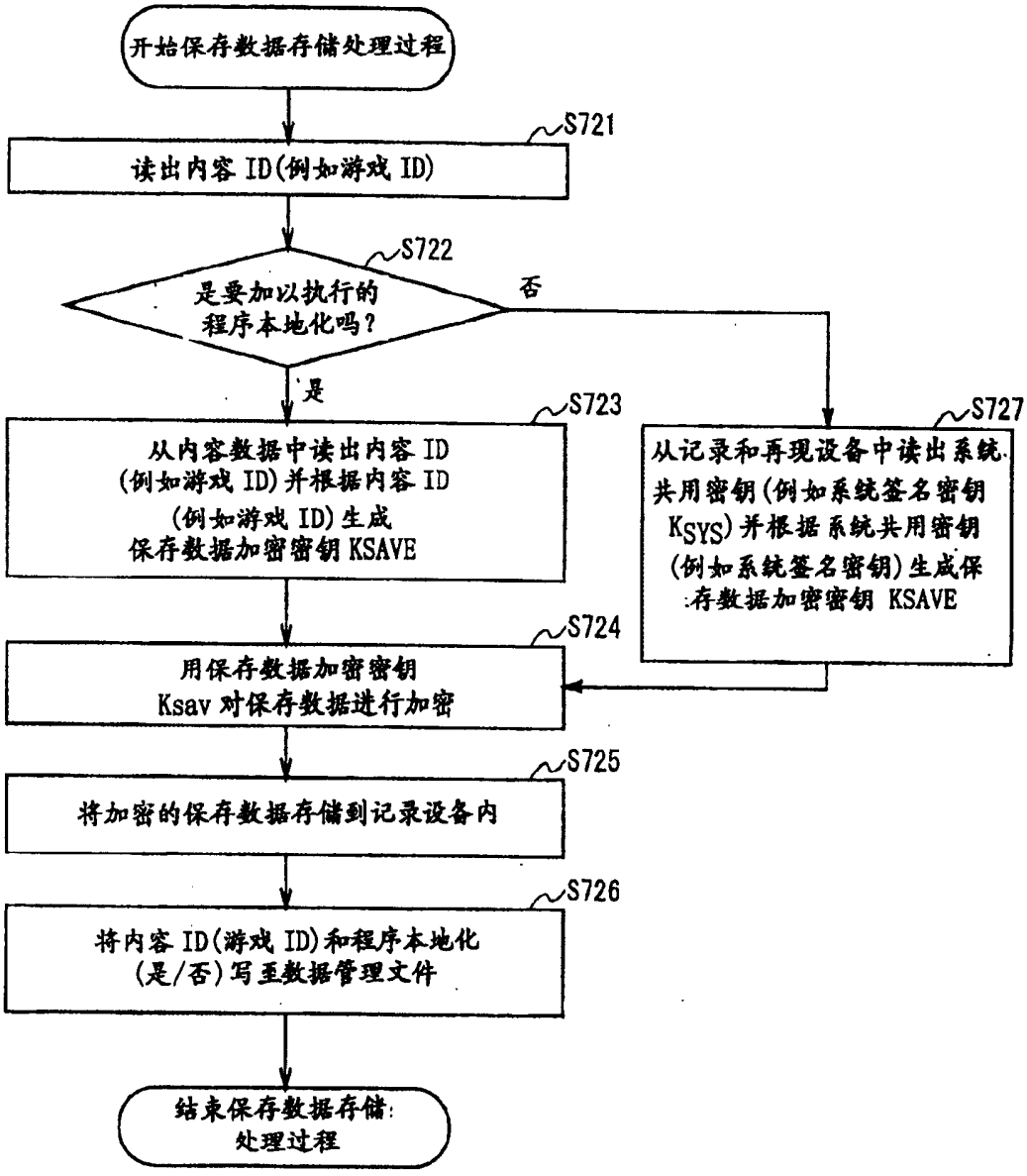


图 73

（4） 用内容 ID 或系统共用密钥的保存数据再现处理过程的实例

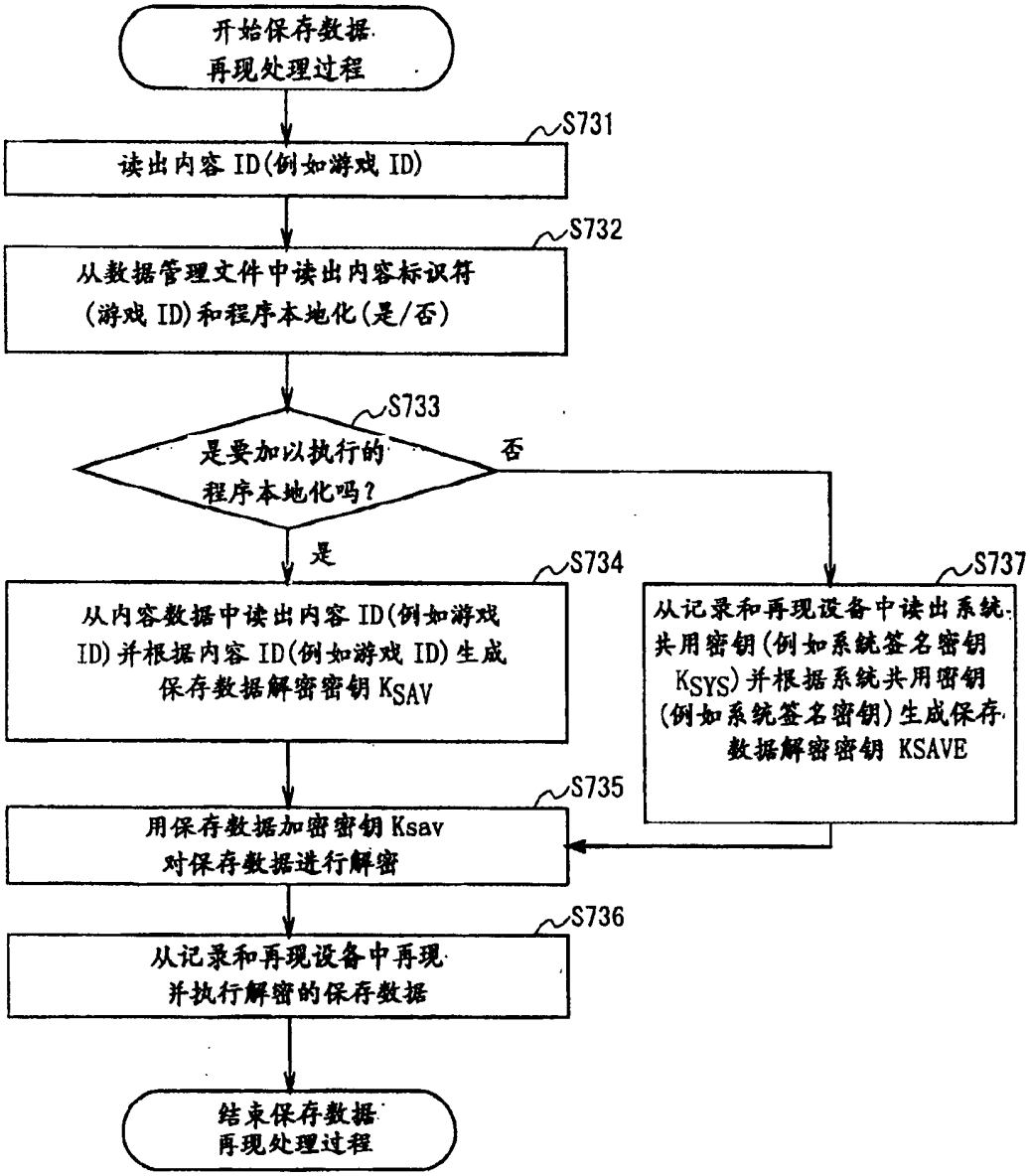


图 74

（5） 用记录和再现设备独有密钥或系统共用密钥的保存数据存储处理过程的实例

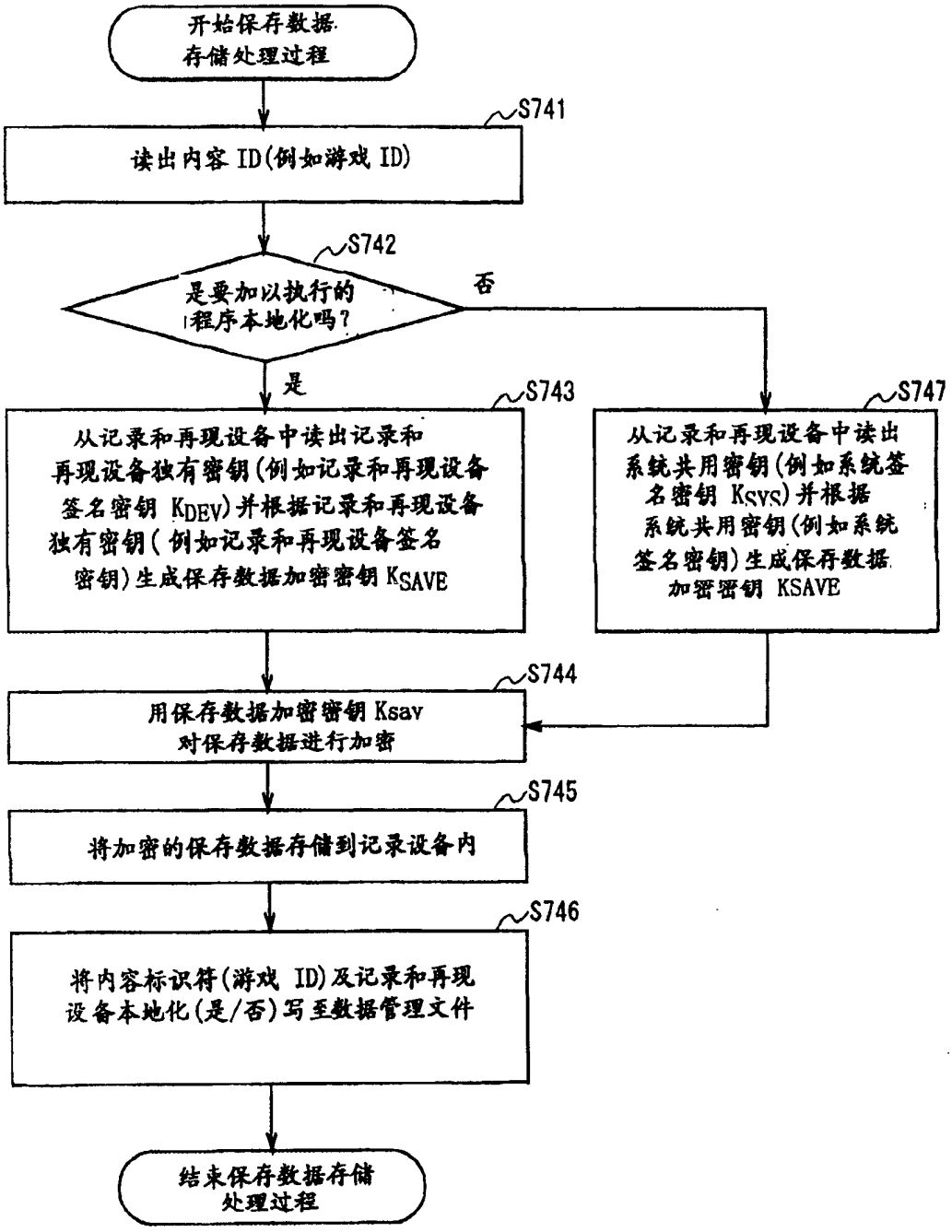


图 75

数据管理文件(2)

数据号	内容 ID(游戏 ID)	记录和再现设备 ID(IDdev)	程序本地化
1	12345678...	56789012...	否
2	ABCDEF12...	09876543...	是
3	12245678...	58834762...	是
⋮	⋮	⋮	⋮

图 76

（6）用记录和再现设备独有密钥或系统共用密钥的保存数据再现处理过程的实例

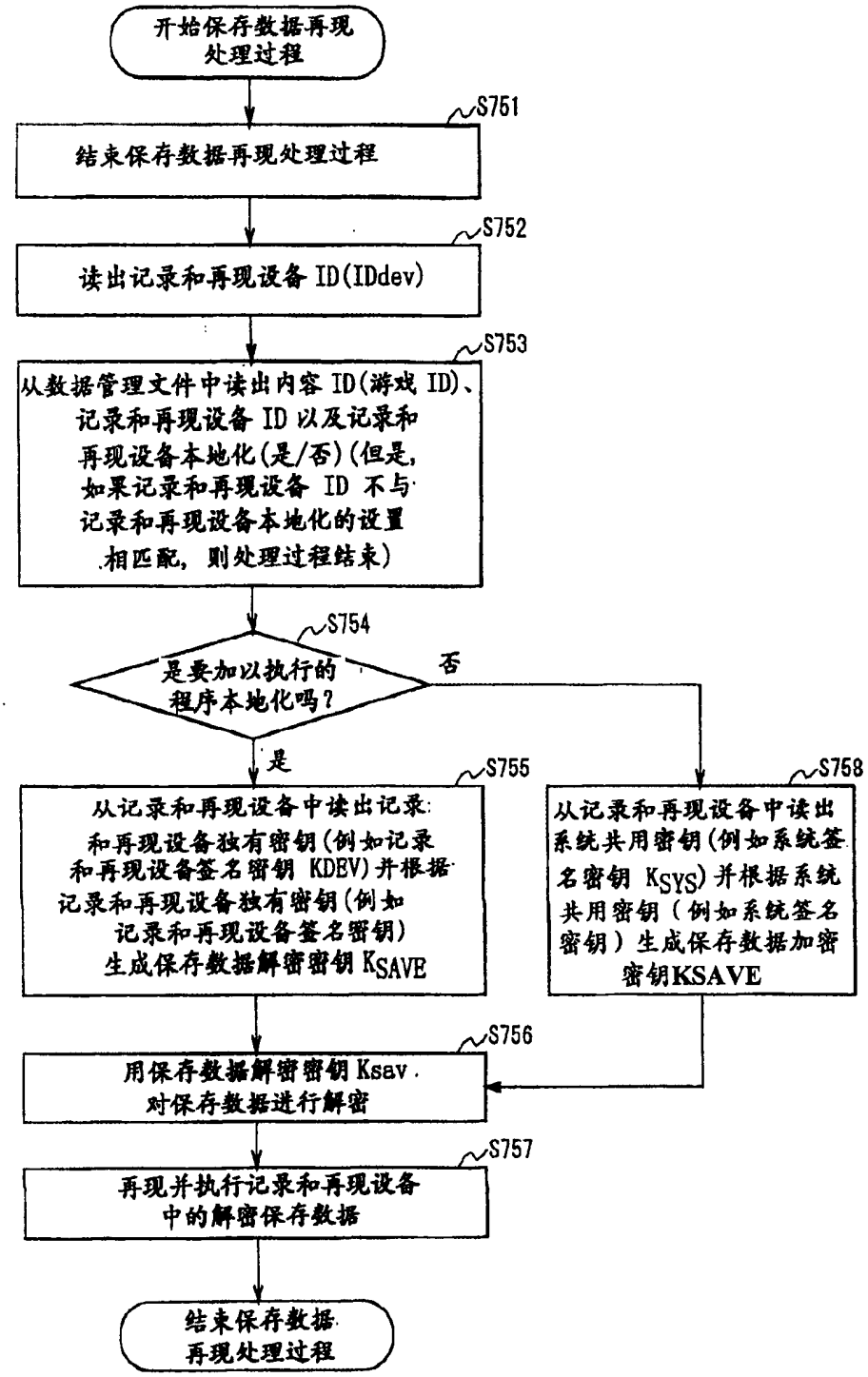


图 77

（7）用记录和再现设备 ID 或系统共用密钥的保存数据存储处理过程的实例

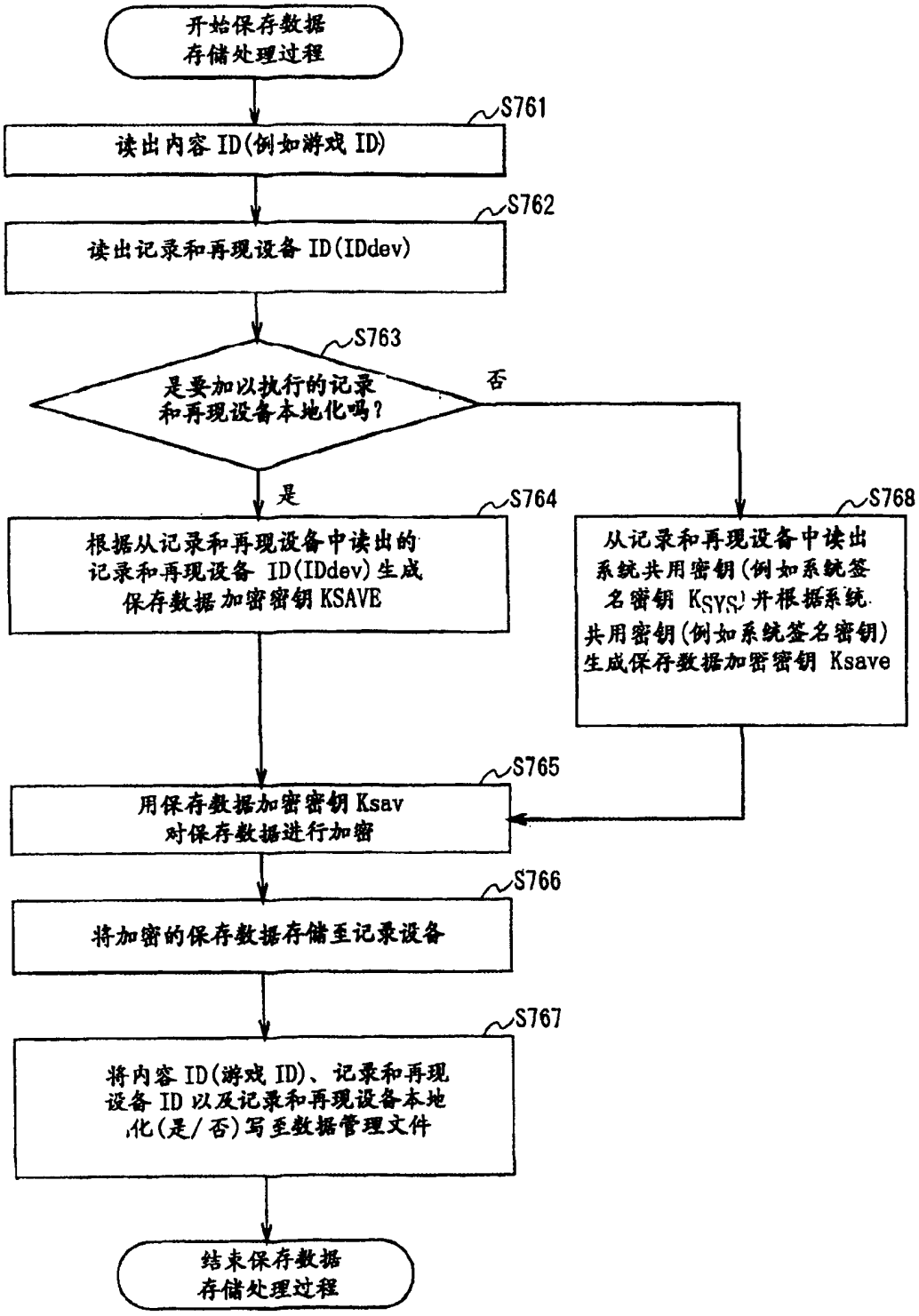


图 78

(8) 用记录和再现设备 ID 或系统共用密钥的保存数据再现处理过程的实例

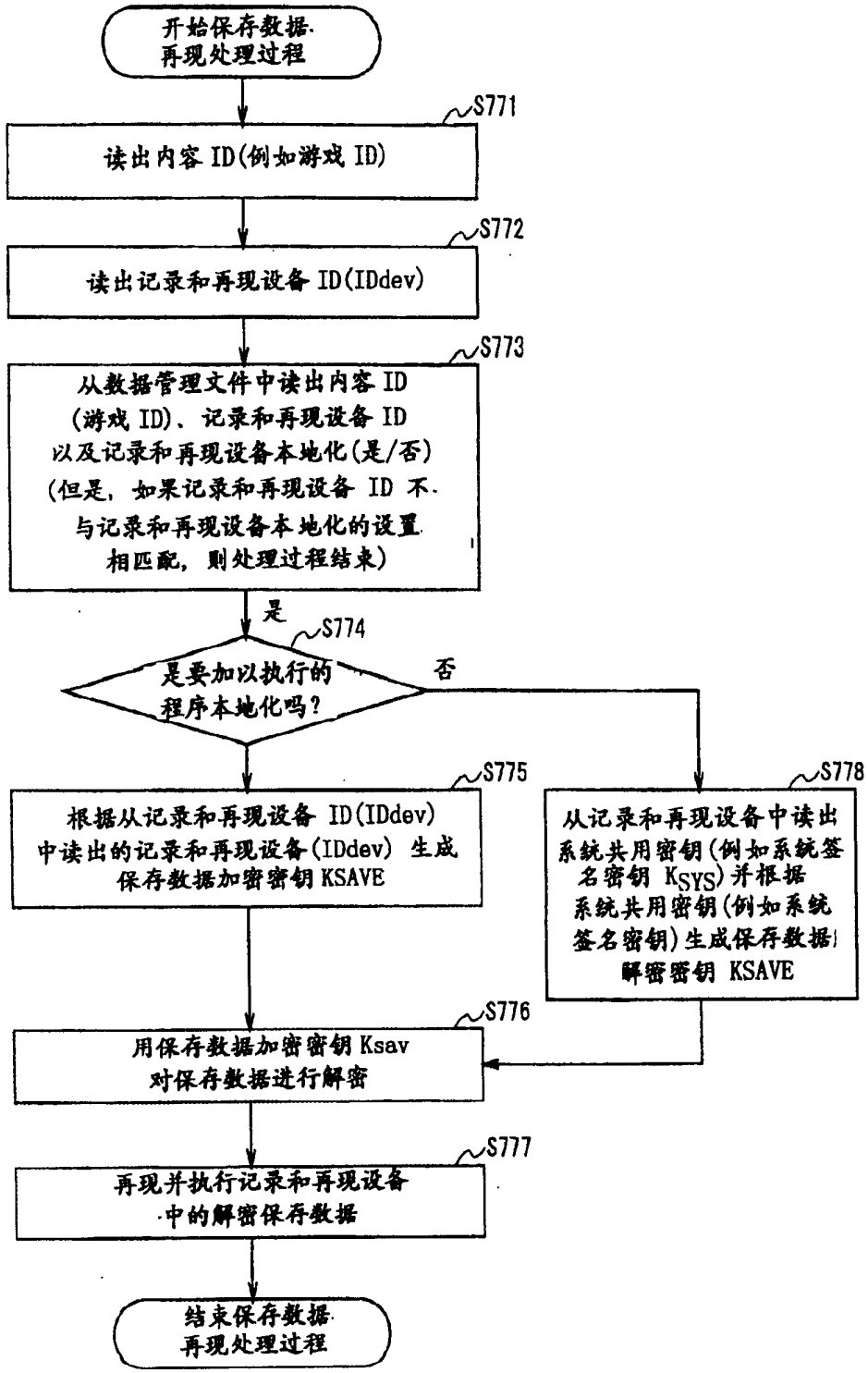


图 79

（9）用内容独有密钥、记录和再现设备独有密钥或系统共用密钥的保存数据存储处理过程的实例

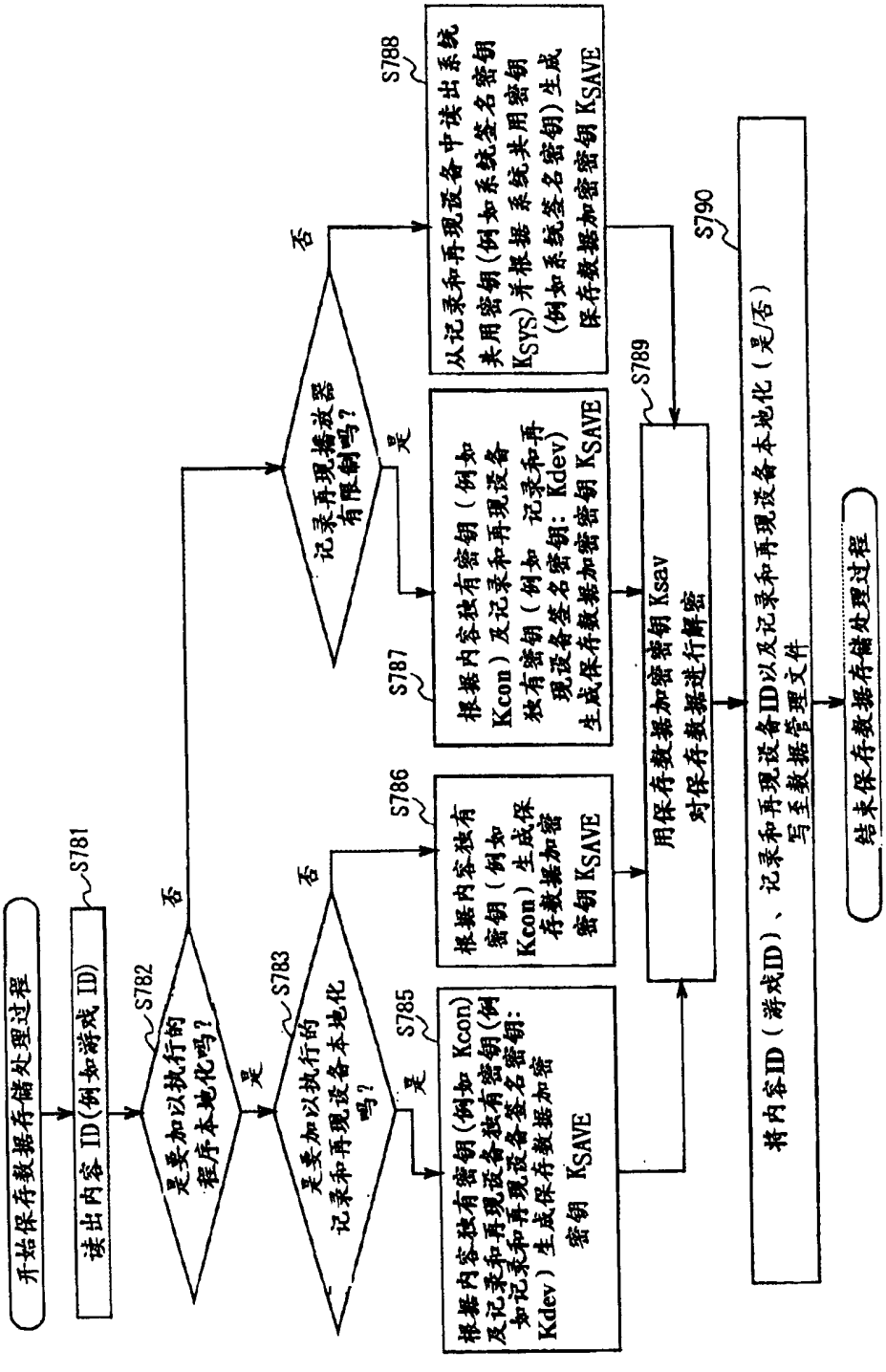


图 80

数据管理文件(3)

数据号	内容 ID (游戏 ID)	记录和再现设备 ID(IDdev)	程序本地化	记录和再现设备本地化
1	123455678...	56789012...	是	否
2	ABCDEF12...	09876543...	是	是
3	1122457678	58834762...	否	是
...	...	...	...	...

图 81

(10) 用内容独有密钥、记录和再现设备独有密钥或系统共用密钥的保存数据再现处理过程的实例

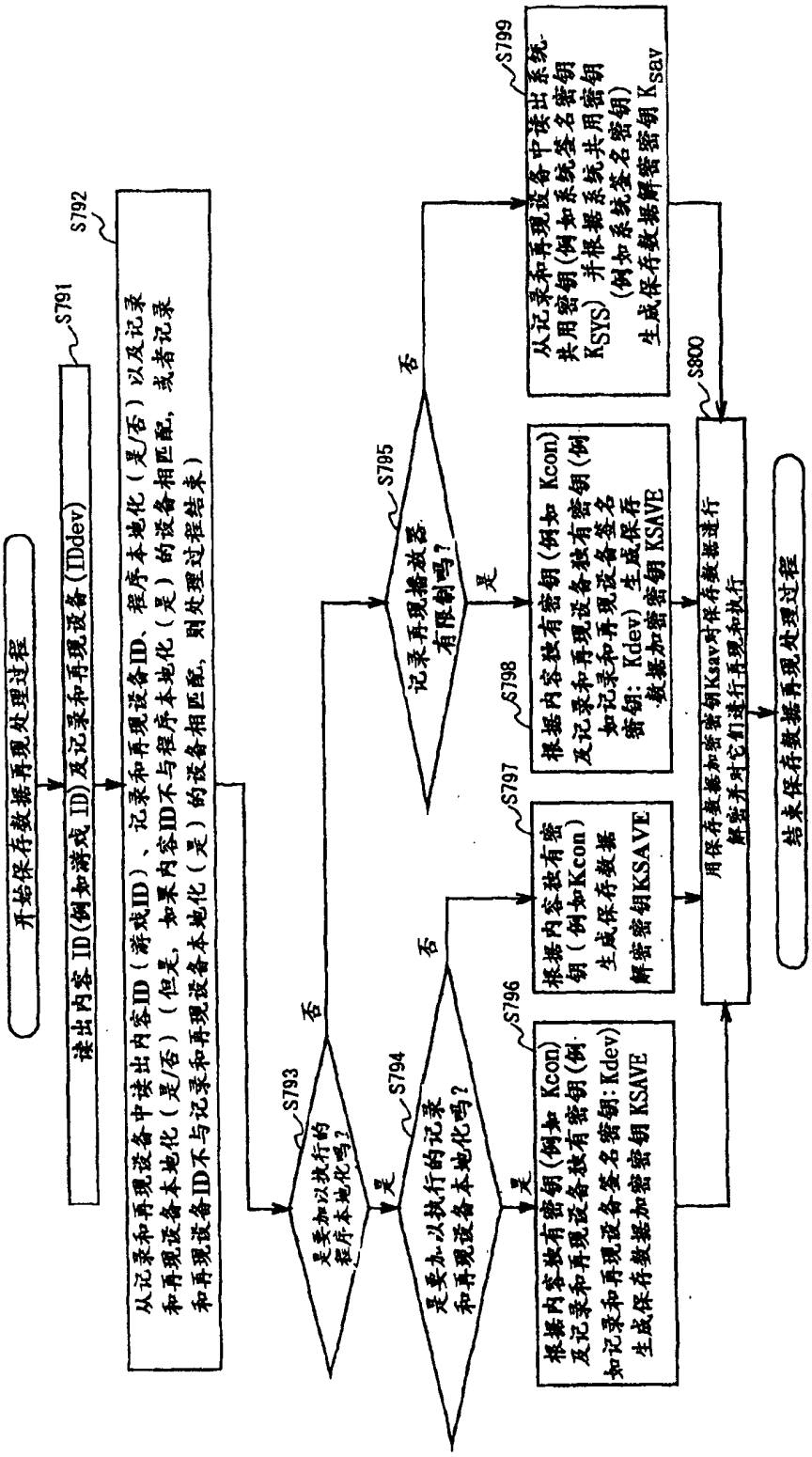


图 82

(11)用用户口令或系统共用密钥的保存数据存储处理过程的实例

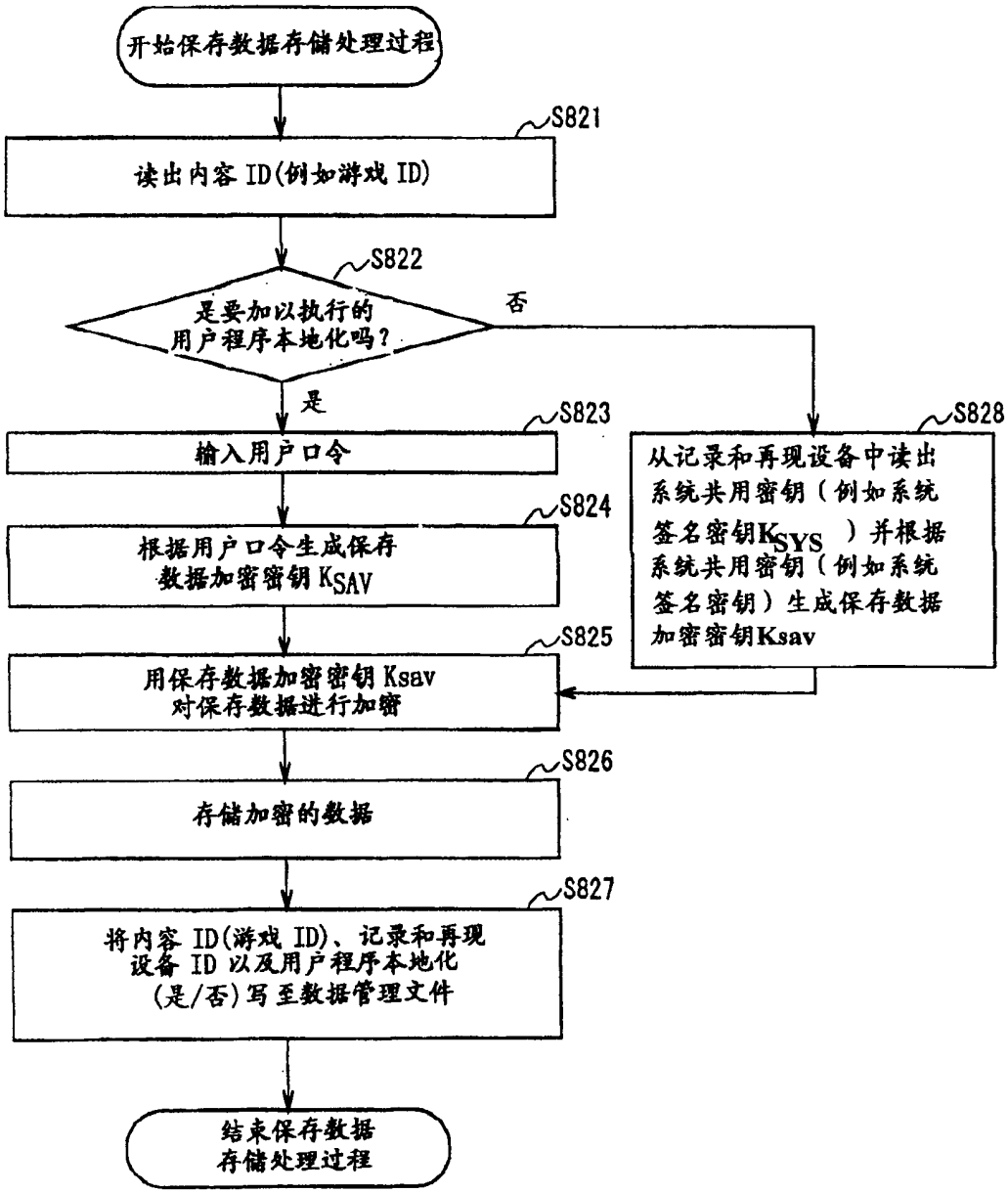


图 83

数据管理文件 (4)

数据号	内容 ID(游戏 ID)	记录和再现设备 ID' (IDdev)	用户程序本地化
1	123455678...	56789012...	是
2	ABCDEF12...	09876543...	是
3	1122457678	58834762...	否
...	...	...	...

图 84

(12) 用用户口令或系统共用密钥的保存数据再现处理过程的实例

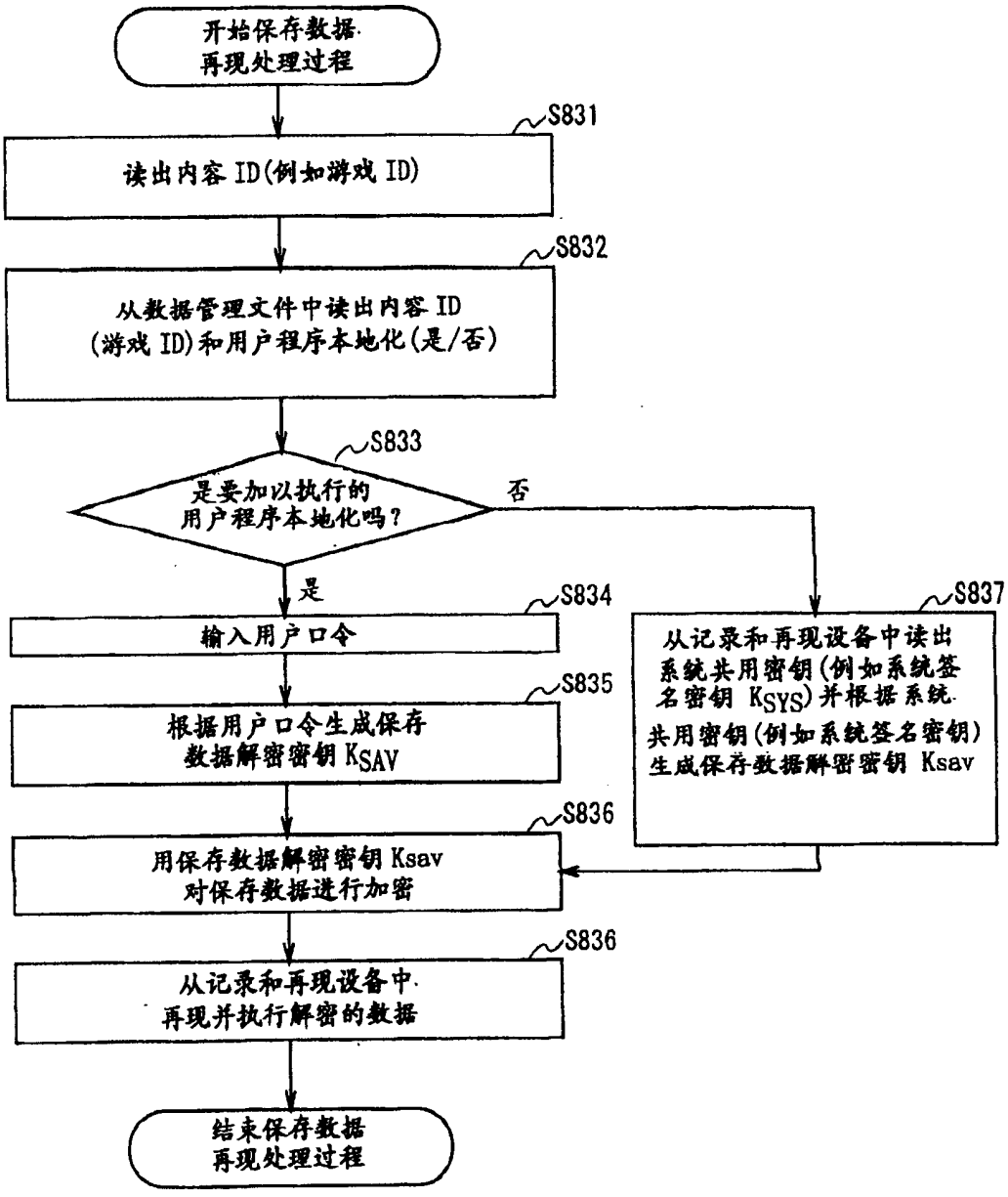


图 85

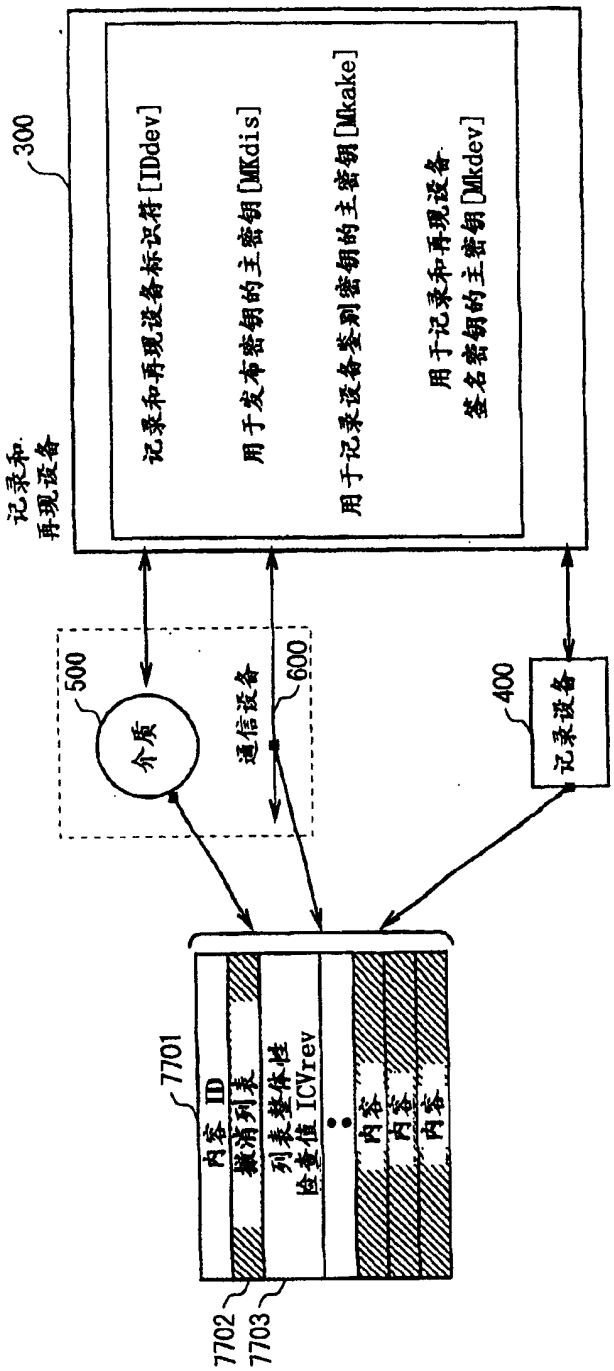

300
记录和再现设备
记录和再现设备标识符[IDdev]
用于发布密钥的主密钥[MKdis]
用于记录设备鉴别密钥的主密钥[Mkake]
用于记录和再现设备签名密钥的主密钥[Mkdev]
500
介质
通信设备
600
400
记录设备
7701
内容 ID
媒体列表
列表整体性检查值 ICVrev
内容
内容
内容
7702
7703

图 86

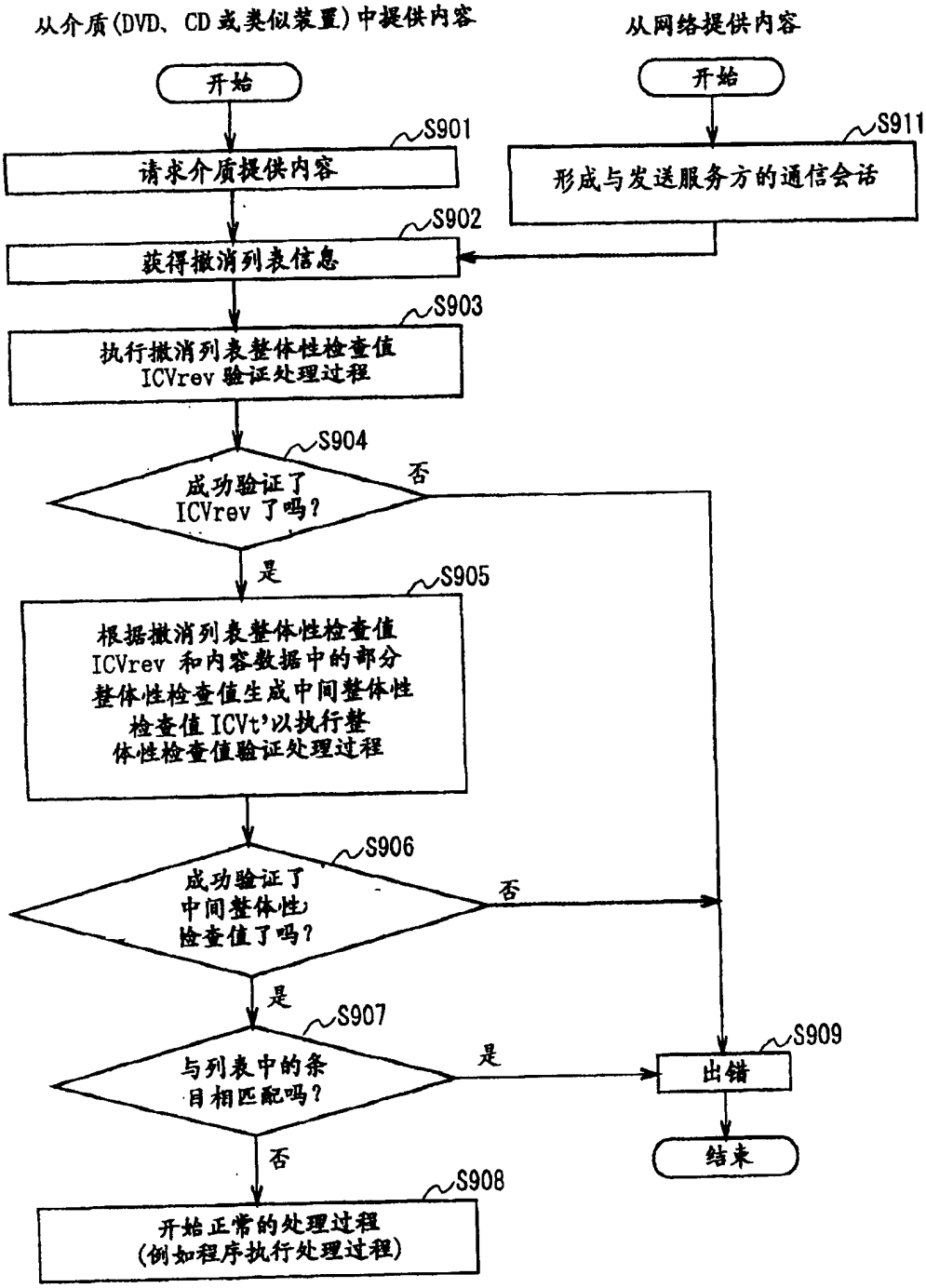

从介质(DVD、CD或类似装置)中提供内容
从网络提供内容
开始
开始
S901
请求介质提供内容
S911
形成与发送服务方的通信会话
S902
获得撤消列表信息
S903
执行撤消列表整体性检查值
ICVrev验证处理过程
S904
成功验证了
ICVrev了吗?
否
是
S905
根据撤消列表整体性检查值
ICVrev和内容数据中的部分
整体性检查值生成中间整体性
检查值ICVt'以执行整
体性检查值验证处理过程
S906
成功验证了
中间整体性
检查值了吗?
否
是
S907
与列表中的条
目相匹配吗?
是
S909
出错
结束
否
S908
开始正常的处理过程
(例如程序执行处理过程)

图 87

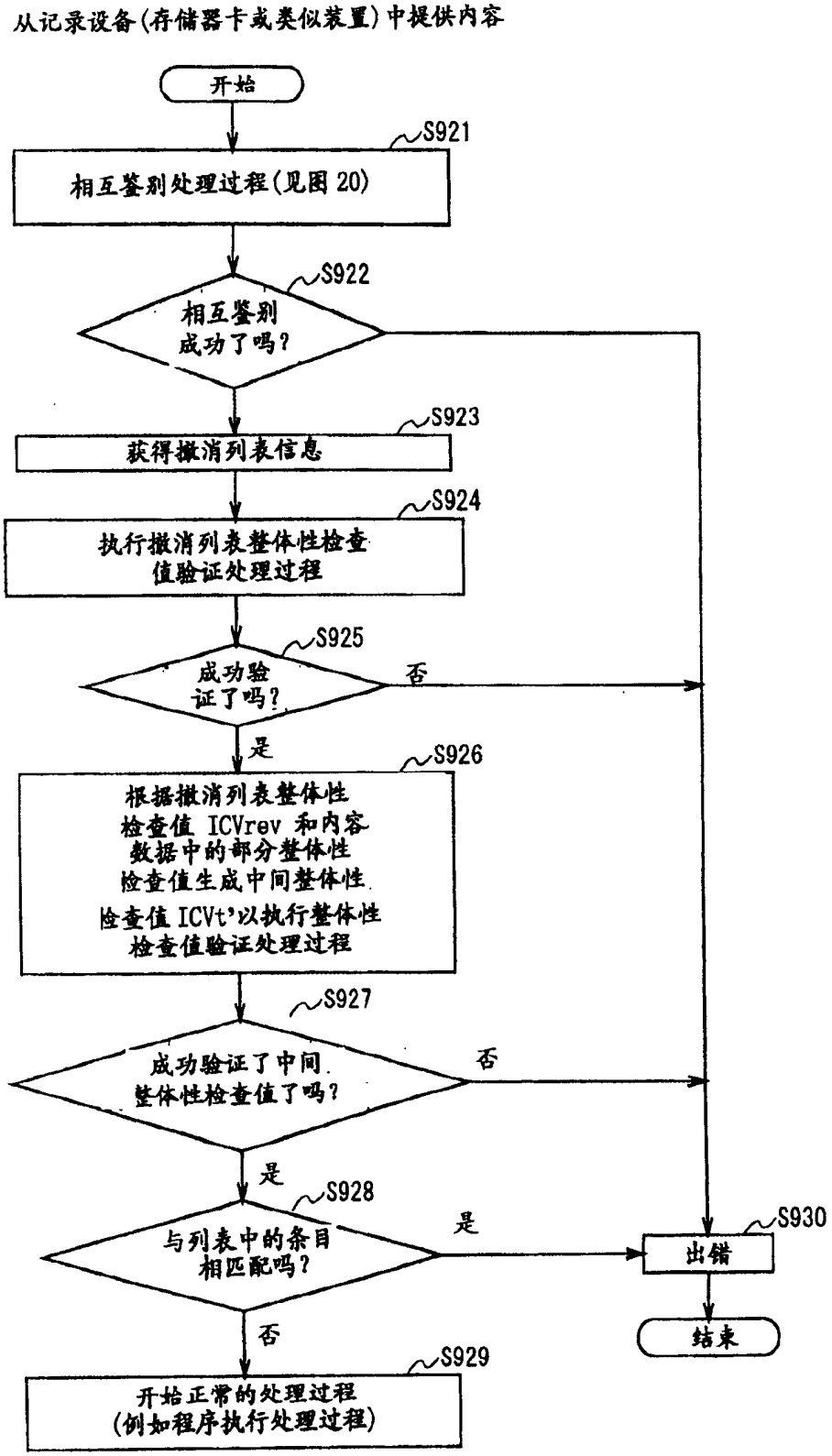

从记录设备(存储器卡或类似装置)中提供内容
开始
S921
相互鉴别处理过程(见图 20)
S922
相互鉴别
成功了吗?
S923
获得撤消列表信息
S924
执行撤消列表整体性检查
值验证处理过程
S925
成功验
证了吗?
否
是
S926
根据撤消列表整体性
检查值 ICVrev 和内容
数据中的部分整体性
检查值生成中间整体性
检查值 ICVt'以执行整体性
检查值验证处理过程
S927
成功验证了中间
整体性检查值了吗?
否
是
S928
与列表中的条目
相匹配吗?
是
S930
出错
结束
否
S929
开始正常的处理过程
(例如程序执行处理过程)

图 88

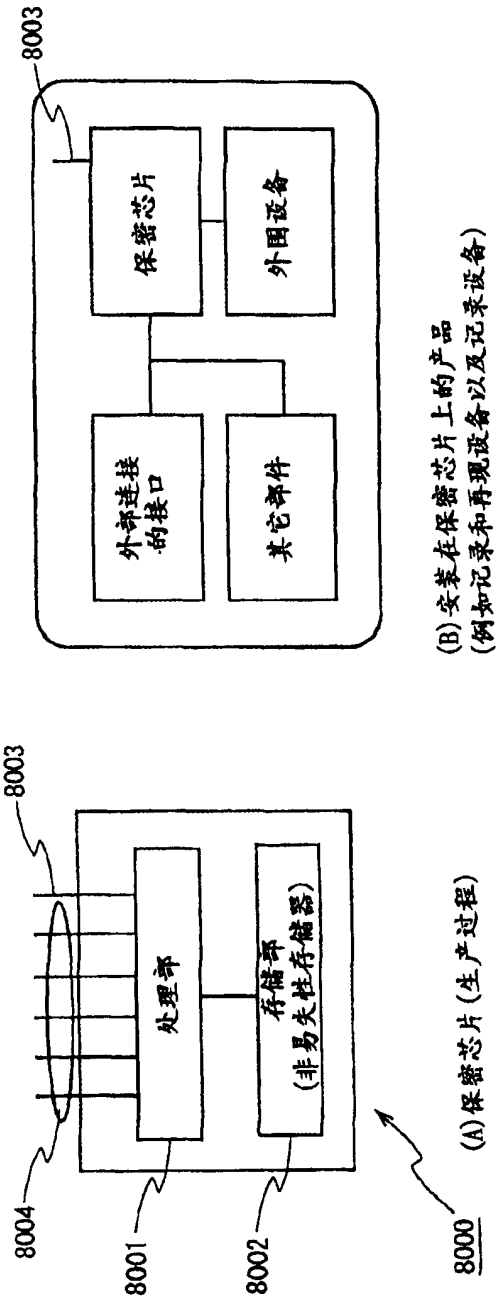

8003
保密芯片
外围设备
外部连接的接口
其它部件
(B)安装在保密芯片上的产品
(例如记录和再现设备以及记录设备)
8003
处理部
存储部
(非易失性存储器)
8004
8001
8002
8000
(A)保密芯片(生产过程)

图 89

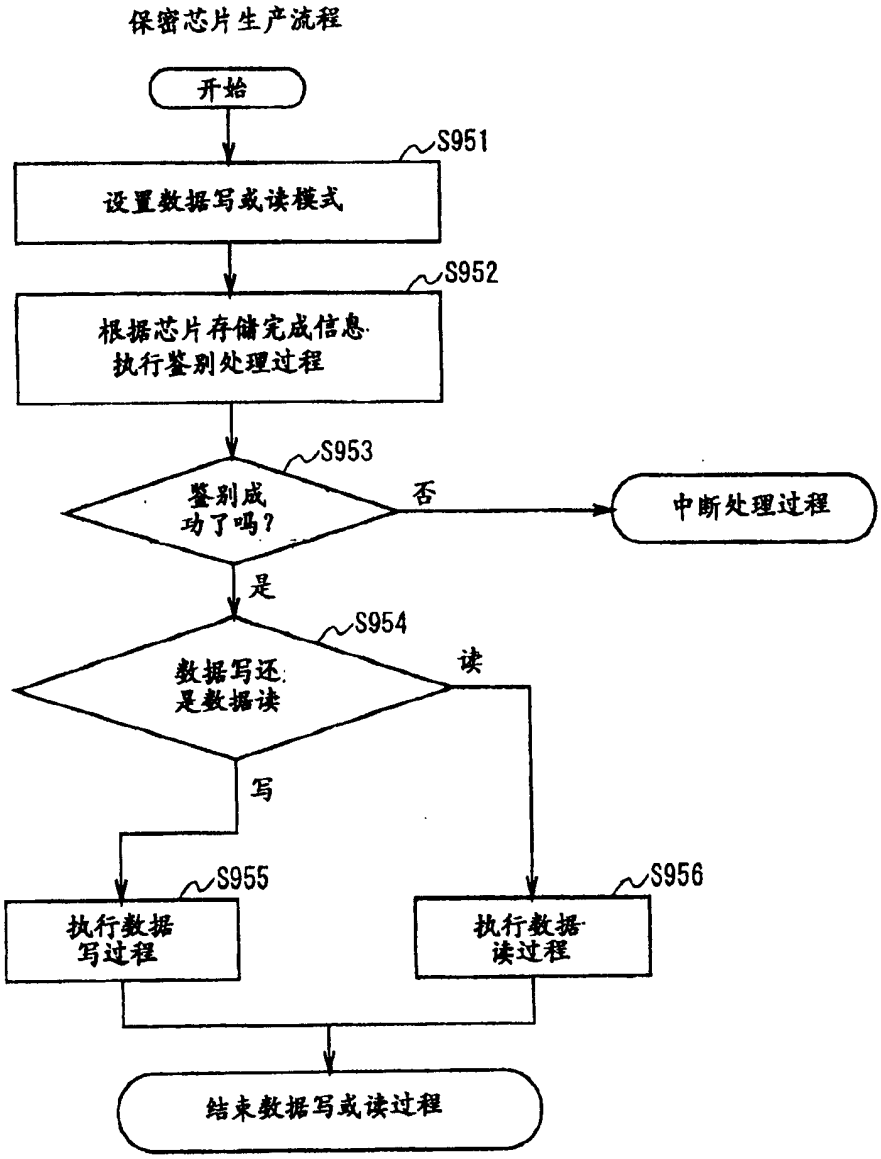

保密芯片生产流程
开始
S951
设置数据写或读模式
S952
根据芯片存储完成信息
执行鉴别处理过程
S953
鉴别成
功了吗?
否
中断处理过程
是
S954
数据写还
是数据读
读
写
S955
执行数据
写过程
S956
执行数据
读过程
结束数据写或读过程

图 90

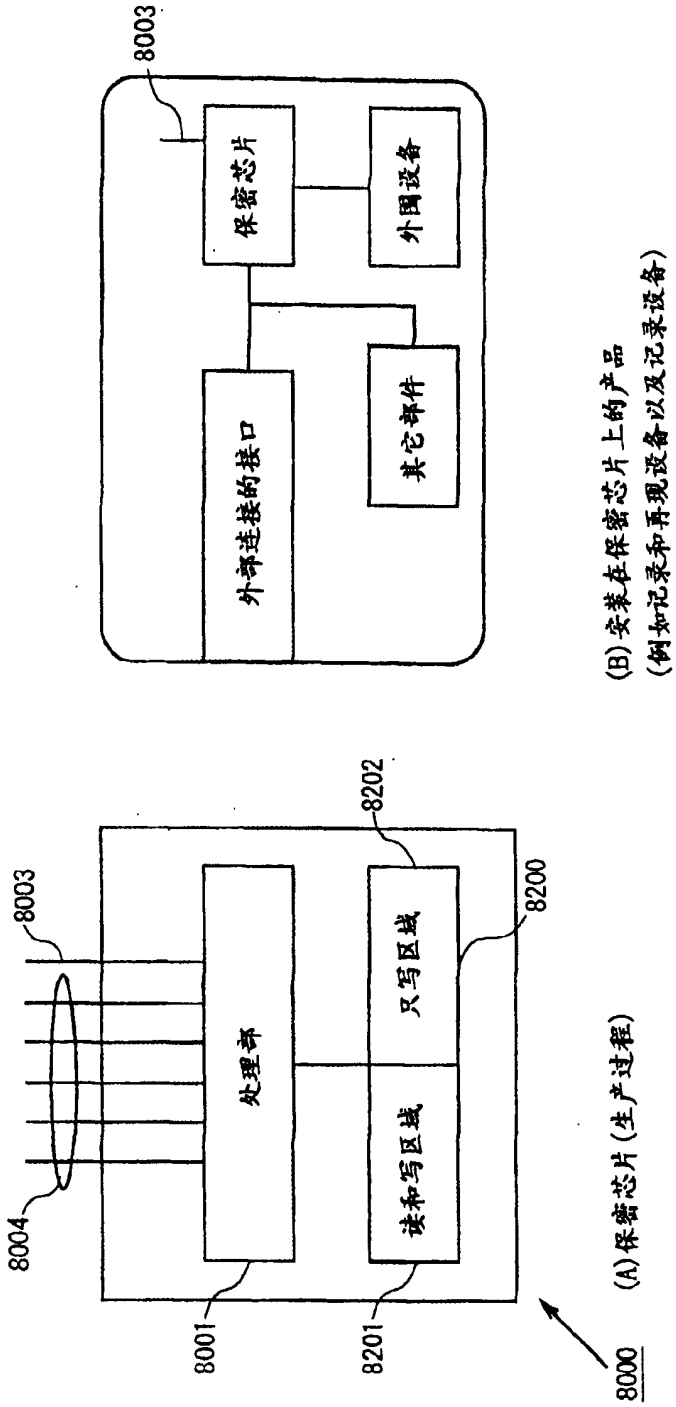

8003
保密芯片
外围设备
外部连接的接口
其它部件
(B)安装在保密芯片上的产品
(例如记录和再现设备以及记录设备)
8202
8003
8200
处理部
只写区域
读和写区域
8004
8001
8201
8000
(A)保密芯片(生产过程)

图 91

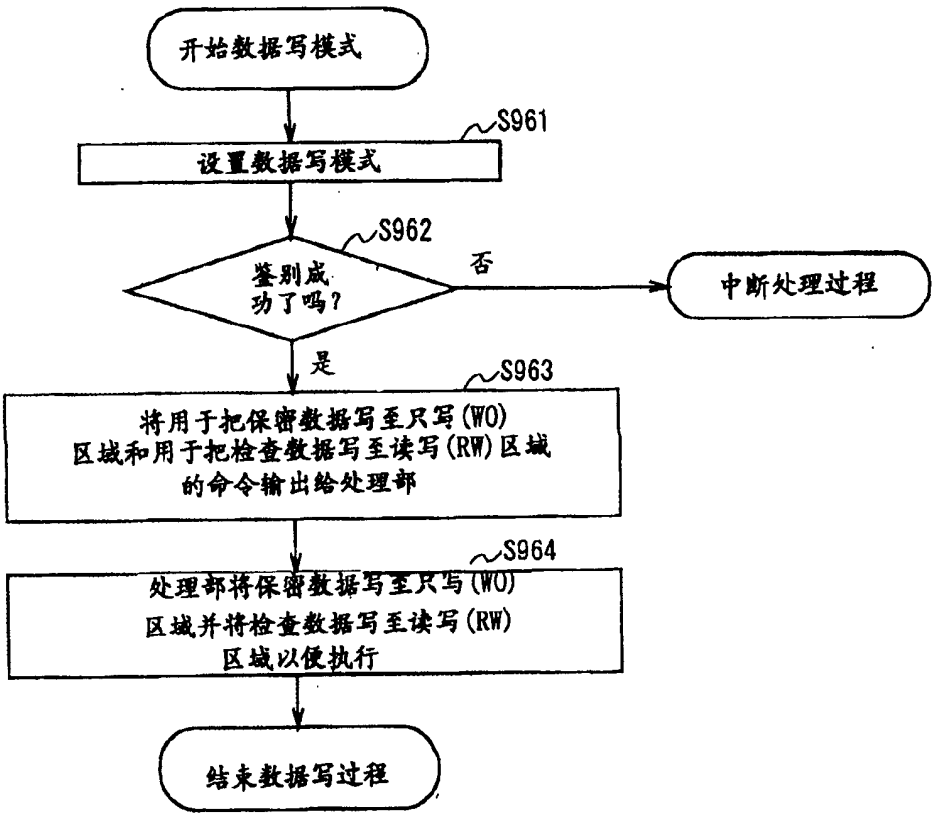

开始数据写模式
S961
设置数据写模式
S962
鉴别成功了吗?
否
中断处理过程
是
S963
将用于把保密数据写至只写(WO)区域和用于把检查数据写至读写(RW)区域的命令输出给处理部
S964
处理部将保密数据写至只写(WO)区域并将检查数据写至读写(RW)区域以便执行
结束数据写过程

图 92

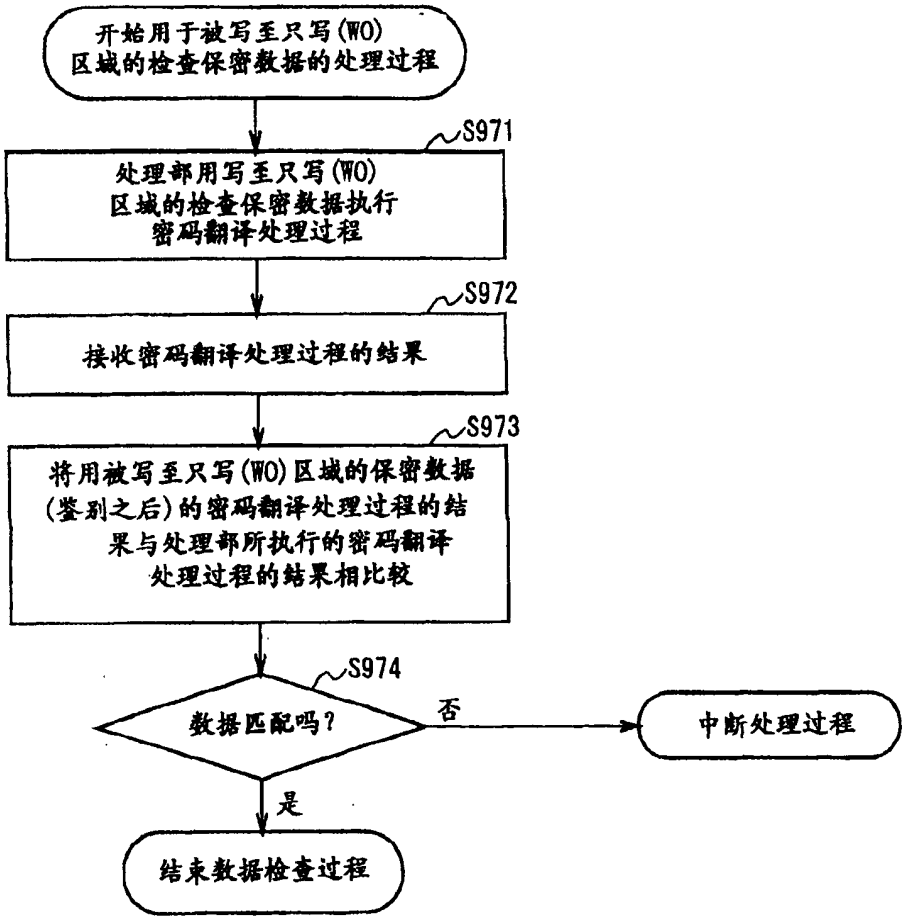

开始用于被写至只写(WO)
区域的检查保密数据的处理过程
S971
处理部用写至只写(WO)
区域的检查保密数据执行
密码翻译处理过程
S972
接收密码翻译处理过程的结果
S973
将用被写至只写(WO)区域的保密数据
(鉴别之后)的密码翻译处理过程的结
果与处理部所执行的密码翻译
处理过程的结果相比较
S974
数据匹配吗?
否
中断处理过程
是
结束数据检查过程

图 93