(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101404167 B
(45)授权公告日 2012.04.18

(21)申请号 200810168231.8

(22)申请日 2008.10.06

(30)优先权数据
2007-258992 2007.10.02 JP

(73)专利权人 索尼株式会社
地址 日本东京都

(72)发明人 久野浩 冈上拓己 藤沼启一

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 李晓冬 南霆

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

(56)对比文件
US 2007011102 A1,2007.01.11, 全文.

审查员 刘欣

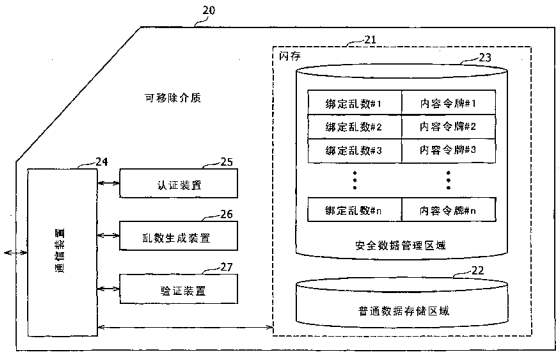
权利要求书 5 页 说明书 20 页 附图 10 页

(54)发明名称

记录系统、信息处理设备、存储设备、记录方法和程序

(57)摘要

本发明提供了记录系统、信息处理设备、存储设备、记录方法和程序。这里公开了一种记录系统，包括：结合有存储介质的存储设备，以及信息处理设备，该信息处理设备可连接到存储设备并且保存要记录到存储设备的内容。




CN 101404167 B

1. 一种记录系统，包括：

结合有存储介质的存储设备，以及

信息处理设备，该信息处理设备可连接到所述存储设备并且保存要记录到所述存储设备的内容，其中所述存储设备是可移除地附接到所述信息处理设备的可移除介质；其中

所述信息处理设备包括：

乱数生成请求部件，该乱数生成请求部件被配置为向所述存储设备发送乱数生成请求；

乱数接收部件，该乱数接收部件被配置为响应于所述乱数生成请求被发送到所述存储设备，从所述存储设备接收构成所述乱数生成请求所特有的变量的乱数；

加密部件，该加密部件被配置为利用从所述存储设备接收的所述乱数对关于所述内容的数据文件进行加密；

数据记录部件，该数据记录部件被配置为将经加密的数据文件记录到所述存储设备的所述存储介质；

散列计算部件，该散列计算部件被配置为计算所述经加密的数据文件的散列值；以及

乱数写入请求部件，该乱数写入请求部件被配置为向所述存储设备发送包括所述散列值的乱数写入请求，

其中所述存储设备包括：

乱数生成请求接收部件，该乱数生成请求接收部件被配置为接收来自所述信息处理设备的乱数生成请求；

乱数生成部件，该乱数生成部件被配置为响应于接收到所述乱数生成请求，生成构成所述乱数生成请求所特有的变量的乱数；

乱数发送部件，该乱数发送部件被配置为将所述乱数发送到所述信息处理设备；

存储介质，该存储介质被配置为存储关于所述内容的数据文件，所述数据文件被所述信息处理设备利用所述乱数进行了加密；

乱数写入请求接收部件，该乱数写入请求接收部件被配置为接收来自所述信息处理设备的包括经加密的数据文件的散列值的乱数写入请求；以及

乱数记录部件，该乱数记录部件被配置为响应于接收到所述乱数写入请求，在将所述乱数写入请求中包括的所述散列值和所述乱数生成部件生成的所述乱数记录到所述存储介质时，将所述散列值和所述乱数关联起来。

2. 根据权利要求 1 所述的记录系统，其中，

在使用存储在所述存储设备中的所述内容时，所述信息处理设备向所述存储设备发送请求从所述存储设备发送所述乱数和所述散列值的发送请求；

在接收到来自所述信息处理设备的所述发送请求时，所述存储设备从所述存储介质读取所述乱数和所述散列值并将所取回的乱数和散列值发送到所述信息处理设备；

所述信息处理设备从所述存储设备获取存储在所述存储介质中的所述经加密的数据文件；并且

所述信息处理设备计算所述经加密的数据文件的散列值，将计算出的散列值与从所述存储设备接收的所述散列值相匹配，并且如果在两个散列值之间存在完全匹配，则利用从所述存储设备接收的所述乱数对所述经加密的数据文件进行解密。

3. 根据权利要求 1 所述的记录系统，其中，

在将所述内容记录到所述存储设备时，所述信息处理设备和所述存储设备相互认证彼此以共享会话密钥；

在向所述存储设备发送所述乱数写入请求时，所述信息处理设备利用所述会话密钥计算所述散列值的消息认证代码值，并且向所述存储设备发送包括所述散列值和从所述散列值得出的所述消息认证代码值的所述乱数写入请求；

在接收到来自所述信息处理设备的所述乱数写入请求时，所述存储设备利用所述会话密钥计算所述乱数写入请求中包括的所述散列值的消息认证代码值，并且如果在计算出的消息认证代码值和所述乱数写入请求中包括的从所述散列值得出的所述消息认证代码值之间存在完全匹配，则在将所述散列值和所述乱数记录到所述存储介质时将所述散列值与所述乱数关联起来。

4. 根据权利要求 3 所述的记录系统，其中，所述信息处理设备和所述存储设备各自利用所述会话密钥计算组合的所述散列值和所述乱数的消息认证代码值。

5. 根据权利要求 1 所述的记录系统，其中

所述存储设备的所述存储介质具有作为存储区域的普通数据存储区域和安全数据管理区域；并且

所述经加密的数据文件被写入到所述普通数据存储区域，并且所述散列值和所述乱数被写入到所述数据管理区域。

6. 根据权利要求 1 所述的记录系统，其中，所述存储设备是被构造成将所述存储介质与被配置为向所述存储介质写入数据和从所述存储介质读取数据的驱动器相集成的内容处理设备。

7. 根据权利要求 1 所述的记录系统，其中，关于所述内容的所述数据文件包括由内容文件、内容密钥文件、标识信息文件和使用条件文件组成的四种文件中的至少一种，所述内容文件具有所述内容，所述内容密钥文件被用于对所述经加密的数据文件进行解密，所述标识信息文件表示用于标识所述内容的标识信息，所述使用条件文件限定使用所述内容的条件。

8. 一种信息处理设备，可连接到结合有存储介质的存储设备并且保存要记录到所述存储设备的内容，其中所述存储设备是可移除地附接到所述信息处理设备的可移除介质，所述信息处理设备包括：

乱数生成请求部件，该乱数生成请求部件被配置为向所述存储设备发送乱数生成请求；

乱数接收部件，该乱数接收部件被配置为响应于所述乱数生成请求被发送到所述存储设备，从所述存储设备接收构成所述乱数生成请求所特有的变量的乱数；

加密部件，该加密部件被配置为利用从所述存储设备接收的所述乱数对关于所述内容的数据文件进行加密；

数据记录部件，该数据记录部件被配置为将经加密的数据文件记录到所述存储设备的所述存储介质；

散列计算部件，该散列计算部件被配置为计算所述经加密的数据文件的散列值；以及

乱数写入请求部件，该乱数写入请求部件被配置为向所述存储设备发送包括所述散列

值的乱数写入请求。

9. 根据权利要求 8 所述的信息处理设备，还包括：

发送请求部件，该发送请求部件被配置为向所述存储设备发送请求从所述存储设备发送所述乱数和所述散列值的发送请求；

管理信息接收部件，该管理信息接收部件被配置为响应于所述发送请求，而从所述存储设备接收存储在所述存储介质中的所述乱数和所述散列值；

数据获取部件，该数据获取部件被配置为从所述存储设备获取存储在所述存储介质中的所述经加密的数据文件；

散列计算部件，该散列计算部件被配置为计算从所述存储设备获取的所述经加密的数据文件的散列值；

散列值匹配部件，该散列值匹配部件被配置为将计算出的散列值与从所述存储设备接收的所述散列值相匹配；以及

解密部件，该解密部件被配置为在两个散列值之间存在完全匹配的情况下利用从所述存储设备接收的所述乱数对所述经加密的数据文件进行解密。

10. 根据权利要求 8 所述的信息处理设备，还包括：

认证部件，该认证部件被配置为与所述存储设备执行相互认证以共享会话密钥；以及

消息认证代码值计算部件，该消息认证代码值计算部件被配置为利用所述会话密钥计算所述散列值的消息认证代码值；其中

所述乱数写入请求部件向所述存储设备发送包括所述散列值和从所述散列值得出的所述消息认证代码值的所述乱数写入请求。

11. 根据权利要求 10 所述的信息处理设备，其中，在计算所述散列值的消息认证代码值时，所述消息认证代码值计算部件利用所述会话密钥计算组合的所述散列值和所述乱数的消息认证代码值。

12. 根据权利要求 8 所述的信息处理设备，其中

所述存储设备的所述存储介质具有作为存储区域的普通数据存储区域和安全数据管理区域；并且

所述经加密的数据文件被写入到所述普通数据存储区域，并且所述散列值和所述乱数被写入到所述数据管理区域。

13. 根据权利要求 8 所述的信息处理设备，其中，关于所述内容的所述数据文件包括由内容文件、内容密钥文件、标识信息文件和使用条件文件组成的四种文件中的至少一种，所述内容文件具有所述内容，所述内容密钥文件被用于对所述经加密的数据文件进行解密，所述标识信息文件表示用于标识所述内容的标识信息，所述使用条件文件限定使用所述内容的条件。

14. 一种存储设备，可连接到信息处理设备并且用于存储由所述信息处理设备保存的内容，其中所述存储设备是可移除地附接到所述信息处理设备的可移除介质，所述存储设备包括：

乱数生成请求接收部件，该乱数生成请求接收部件被配置为接收来自所述信息处理设备的乱数生成请求；

乱数生成部件，该乱数生成部件被配置为响应于接收到所述乱数生成请求，生成构成

所述乱数生成请求所特有的变量的乱数；

乱数发送部件，该乱数发送部件被配置为将所述乱数发送到所述信息处理设备；

存储介质，该存储介质被配置为存储关于所述内容的数据文件，所述数据文件被所述信息处理设备利用所述乱数进行了加密；

乱数写入请求接收部件，该乱数写入请求接收部件被配置为接收来自所述信息处理设备的包括经加密的数据文件的散列值的乱数写入请求；以及

乱数记录部件，该乱数记录部件被配置为响应于接收到所述乱数写入请求，在将所述乱数写入请求中包括的所述散列值和所述乱数生成部件生成的所述乱数记录到所述存储介质时，将所述散列值和所述乱数关联起来。

15. 根据权利要求 14 所述的存储设备，还包括：

发送请求接收部件，该发送请求接收部件被配置为从所述信息处理设备接收请求向所述信息处理设备发送存储在所述存储介质中的所述乱数和所述散列值的发送请求；以及

管理信息发送部件，该管理信息发送部件被配置为响应于接收到所述发送请求，读出存储在所述存储介质中的所述乱数和所述散列值并向所述信息处理设备发送。

16. 根据权利要求 14 所述的存储设备，还包括：

认证部件，该认证部件被配置为与所述信息处理设备执行相互认证以共享会话密钥，其中

所述乱数写入请求接收部件接收包括所述散列值和由所述信息处理设备利用所述会话密钥计算出的所述散列值的消息认证代码值的所述乱数写入请求；

所述存储设备还包括

验证部件，该验证部件被配置为响应于接收到所述乱数写入请求，利用所述会话密钥计算所述乱数写入请求中包括的所述散列值的消息认证代码值，以便验证在计算出的消息认证代码值和所述乱数写入请求中包括的所述散列值的消息认证代码值之间是否存在完全匹配；并且

如果在两个消息认证代码值之间存在完全匹配，则所述乱数记录部件在将所述散列值和所述乱数记录到所述存储介质时将所述散列值与所述乱数关联起来。

17. 根据权利要求 16 所述的存储设备，其中，在计算所述散列值的消息认证代码值时，所述验证部件利用所述会话密钥计算组合的所述散列值和所述乱数的消息认证代码值。

18. 根据权利要求 14 所述的存储设备，其中

所述存储设备的所述存储介质具有作为存储区域的普通数据存储区域和安全数据管理区域；并且

所述经加密的数据文件被写入到所述普通数据存储区域，并且所述散列值和所述乱数被写入到所述数据管理区域。

19. 根据权利要求 14 所述的存储设备，其中，所述存储设备是被构造成将所述存储介质与被配置为向所述存储介质写入数据和从所述存储介质读取数据的驱动器相集成的内容处理设备。

20. 根据权利要求 14 所述的存储设备，其中，关于所述内容的所述数据文件包括由内容文件、内容密钥文件、标识信息文件和使用条件文件组成的四种文件中的至少一种，所述内容文件具有所述内容，所述内容密钥文件被用于对所述经加密的数据文件进行解密，所

述标识信息文件表示用于标识所述内容的标识信息，所述使用条件文件限定使用所述内容的条件。

21. 一种用于结合信息处理设备使用的记录方法，该信息处理设备可连接到结合有存储介质的存储设备并且保存要记录到所述存储设备的内容，其中所述存储设备是可移除地附接到所述信息处理设备的可移除介质，所述记录方法包括以下步骤：

在向所述存储设备记录所述内容时，向所述存储设备发送乱数生成请求；

响应于所述乱数生成请求被发送到所述存储设备，从所述存储设备接收构成所述乱数生成请求所特有的变量的乱数；

利用从所述存储设备接收的所述乱数对关于所述内容的数据文件进行加密；

将经加密的数据文件记录到所述存储设备的所述存储介质；

计算所述经加密的数据文件的散列值；以及

向所述存储设备发送包括所述散列值的乱数写入请求，使得所述存储设备在将所述散列值和所述乱数记录到所述存储介质时将所述散列值与所述乱数关联起来。

22. 一种用于结合存储设备使用的记录方法，该记录设备可连接到信息处理设备并且用于存储由所述信息处理设备保存的内容，其中所述存储设备是可移除地附接到所述信息处理设备的可移除介质，所述记录方法包括以下步骤：

接收来自所述信息处理设备的乱数生成请求；

响应于接收到所述乱数生成请求，生成构成所述乱数生成请求所特有的变量的乱数；

将所述乱数发送到所述信息处理设备；

向所述存储介质记录关于所述内容的数据文件，所述数据文件被所述信息处理设备利用所述乱数进行了加密；

接收来自所述信息处理设备的包括经加密的数据文件的散列值的乱数写入请求；以及

响应于接收到所述乱数写入请求，在将所述乱数写入请求中包括的所述散列值和在所述乱数生成步骤中生成的所述乱数记录到所述存储介质时，将所述散列值和所述乱数关联起来。

# 记录系统、信息处理设备、存储设备、记录方法和程序

## 技术领域

[0001] 本发明涉及记录系统、信息处理设备、存储设备、记录方法和程序。

## 背景技术

[0002] 近年来，以蓝光光盘 (Blu-ray Disk，注册商标；简称为 BD) 和 HDDVD( 高清晰度 DVD) 为代表的大容量存储光盘已经采用了一种被称为 AACS( 高级访问内容系统 ) 的用来将内容安全地记录在存储介质上的著作权保护技术 ( 参见 2006 年 8 月 2 日建立、2007 年 9 月 1 日搜索到的因特网上“http://www.aacsla.com/specifications/”处的“AACS Homepage[online]”)。在 AACS 方案中，要记录在诸如 BD 之类的大容量存储光盘上的内容被以禁止其非法拷贝或倒卷 (rewind) 的方式进行了控制。对内容进行倒卷指的是对记录到存储介质的关于其上写入的所述内容的信息 ( 例如，允许的拷贝次数、允许的再现次数 ) 进行初始化，以便对该内容进行非法使用。

[0003] AACS 规范定义了用来将内容写入到诸如光盘之类的存储介质的内容记录方法。根据其规范，AACS 提供了以下的主要特征 :

[0004] (1) 提供了每个存储介质所特有的介质 ID。介质 ID 秘密地与内容密钥相关联。此特征旨在防止介质间内容的非法拷贝。

[0005] (2) 每次内容及其内容密钥被记录到一个介质时，驱动所述介质的介质驱动器就生成绑定乱数 (binding nonce，简称为 BN)，该绑定乱数是可丢弃的随机数据。主机设备接收 BN，利用 BN 对内容密钥进行加密，并且将经加密的内容密钥与 BN 一起写入到介质。此特征使得可以在每次向每件介质记录一内容时向该介质记录 ( 即绑定 ) 内容密钥，从而禁止了对所述内容的非法倒卷。

[0006] 图 1 示意性地示出了在传统的 AACS 方案中内容密钥被写入到诸如 BD 之类的介质的步骤。在步骤 S1 中，主机设备和介质驱动器相互认证彼此。在步骤 S2 中，主机设备从介质驱动器获取介质 ID。在步骤 S3 中，主机设备请求介质驱动器生成 BN。介质驱动器在步骤 S4 中生成新的 BN 并在步骤 S5 中将其发送到主机设备。在步骤 S6 中，主机设备利用介质 ID、BN 和介质密钥区块 (MKB) 对内容密钥 ( 也被称为标题密钥 ) 进行加密。在步骤 S7 中，主机设备将许可证 (license) 和经加密的内容密钥文件写入到该介质。在步骤 S8 中，介质驱动器将从主机设备接收的内容密钥文件和早先在步骤 S4 中生成的 BN 两者写入到该介质。例如，如果所述的介质是 BD，则介质驱动器将 BN 写入到 CPS 标题密钥文件的扇区头部。在传统的遵循 AACS 的光盘上，诸如内容密钥文件之类的数据文件和 BN 都被写入到同一扇区以将两者与彼此关联起来，如上所述。

## 发明内容

[0007] 应当注意，传统的 AACS 规范仅适用于诸如 BD 之类的光盘，并且 BN 是由光盘驱动器生成的。已经假定，存在一种设备 ( 例如光盘驱动器 )，其能够实现与主机设备的相互认证，并且能够将内容和 BN 相结合地安全记录到盘。换言之，传统的 AACS 规范没有预料到结

合了闪存等等的存储卡的使用。

[0008] 蓝光光盘是这样一种方案的一部分：在该方案下，向其记录数据的位置的逻辑地址在记录之前就被指定。在所使用的介质是 BD 的情况下，内容密钥文件和 BN 在图 1 的步骤 S8 中被同时记录。在这种情况下，向其写入文件的目的地位置的逻辑地址早在步骤 S3 中就被指定。文件和 BN 都需要同时被写入到该指定的地址。也就是说，传统的使用 BN 的记录方案非常依赖于介质（例如 BD）的物理格式。如果记录系统依赖于介质的物理格式，那么就有可能会出现以下两个主要缺点：

[0009] (A) 记录系统不适合于以文件为单位进行访问的介质。

[0010] 一些存储介质服从诸如 PTP（图片传输协议）或 MTP（媒体传输协议）之类的按文件访问（文件级访问）协议。当要利用上述使用 BD 的记录方案来将数据记录到该类介质时，通常必须遵守构成记录过程的以下序列 (1) 至 (3)：

[0011] (1) 主机设备从介质驱动器获取用于写入内容密钥文件的介质 ID（相当于地址）。

[0012] (2) 在介质 ID 被指定的情况下，主机设备使得介质驱动器相应地生成 BN。

[0013] (3) 介质驱动器确定内容密钥文件被利用介质 ID 记录到该介质。在内容密钥文件被记录时，介质驱动器将 BN 写入到该介质。

[0014] 对遵循以上记录过程的需要降低了在出于访问目的按文件放入或取得数据时的自由度。例如，可能无法以时间上交错的方式首先仅记录内容密钥文件并随后写入 BN。

[0015] 当该介质上记录的内容密钥文件被改变或删除时，相应的 BN 必须也被删除。总是需要特殊的布置来将每个内容密钥文件与有关 BN 关联起来，这又可能是另一个不便之处。更具体而言，在所使用的存储介质是 BD 的情况下，文件和 BN 被记录在同一扇区中，因而易于根据需要被同时删除。如果存储介质是通常结合有闪存的存储卡，则 BN 需要与文件相分开地被写入到特别分配的管理区域。这需要提供特殊的布置，来不断地检查以了解是否有任何文件被改变或删除，使得任何被改变或删除的文件都必须与相应被无效的 BN 相匹配。

[0016] (B) 要记录的文件的格式变得依赖于记录格式。

[0017] 在传统的用于 BD 的记录方案中，在 BN 被生成之前，主机设备需要知道向其写入内容密钥文件的地址。这意味着要记录的文件的格式变得依赖于要记录在介质上的内容密钥文件的记录格式。这个要求在多种情况中伴随着不便之处。例如，可能希望在介质上创建一巨大的文件，使得该文件可以被用作向其记录内容密钥文件和内容的虚拟文件系统。又例如，可能希望在内容密钥文件和内容被记录之前将其压缩成单个文件。在这种情况下，可能无法预先知道在介质上向其写入任何内容密钥文件的地址。这意味着难以利用传统的记录方案来将文件记录在 BD 上。换言之，传统的使用 BD 的记录方案未能应对这样的情况，即诸如包含多个内容密钥的盘镜像之类的大量数据要作为单个文件被记录。传统上，可能无法依据所关注的应用来根据需要切换记录系统。

[0018] 本发明的实施例是考虑到上述情况而作出的，并且提供了具有新颖的改进的记录系统、信息处理设备、存储设备、记录方法和程序，用于允许内容被安全地记录，而不会变得依赖于存储介质的物理格式。

[0019] 在执行本发明时，根据其一个实施例，提供了一种记录系统，包括：结合有存储介质的存储设备，以及信息处理设备，该信息处理设备可连接到存储设备并且其中保存了要记录到存储设备的内容。在将内容记录到存储设备时，信息处理设备向存储设备发送乱数

生成请求。在接收到来自信息处理设备的乱数生成请求时，存储设备生成构成乱数生成请求所特有的变量的乱数并将所生成的乱数发送到信息处理设备。利用从存储设备接收的乱数，信息处理设备对关于内容的数据文件进行加密并将经加密的数据文件记录到存储设备的存储介质。信息处理设备计算经加密的数据文件的散列值 (hash value) 并向存储设备发送包括散列值的乱数写入请求。在接收到来自信息处理设备的乱数写入请求时，存储设备将散列值与乱数关联起来并将散列值和乱数记录到存储介质。

[0020] 优选地，在使用存储在存储设备中的内容时，信息处理设备可以向存储设备发送请求从存储设备发送乱数和散列值的发送请求。在接收到来自信息处理设备的发送请求时，存储设备可以从存储介质读取乱数和散列值并将所取回的乱数和散列值发送到信息处理设备。信息处理设备可以从存储设备获取存储在存储介质中的经加密的数据文件。信息处理设备可以计算经加密的数据文件的散列值，将计算出的散列值与从存储设备接收的散列值相匹配，并且如果在两个散列值之间存在完全匹配，则利用从存储设备接收的乱数对经加密的数据文件进行解密。

[0021] 优选地，在将内容记录到存储设备时，信息处理设备和存储设备可以相互认证彼此以共享会话密钥。在向存储设备发送乱数写入请求时，信息处理设备可以利用会话密钥计算散列值的 MAC（消息认证代码）值，并且可以向存储设备发送包括散列值和从散列值得出的 MAC 值的乱数写入请求。在接收到来自信息处理设备的乱数写入请求时，存储设备可以利用会话密钥计算乱数写入请求中包括的散列值的 MAC 值，并且如果在计算出的 MAC 值和乱数写入请求中包括的从散列值得出的 MAC 值之间存在完全匹配，则可以在将散列值和乱数记录到存储介质时将散列值与乱数关联起来。

[0022] 优选地，信息处理设备和存储设备可以各自利用会话密钥计算组合的散列值和乱数的 MAC 值。

[0023] 优选地，存储设备的存储介质可以具有作为存储区域的普通数据存储区域和安全数据管理区域。经加密的数据文件可以被写入到普通数据存储区域，并且散列值和乱数可以被写入到数据管理区域。

[0024] 优选地，存储设备可以是可移除地附接到信息处理设备的可移除介质。

[0025] 优选地，存储设备可以是被构造成将存储介质与被配置为向存储介质写入数据和从存储介质读取数据的驱动器相集成的内容处理设备。

[0026] 优选地，关于内容的数据文件可以包括由内容文件、内容密钥文件、标识信息文件和使用条件文件组成的四种文件中的至少一种，内容文件中具有内容，内容密钥文件被用于对经加密的数据文件进行解密，标识信息文件表示用于标识内容的标识信息，使用条件文件限定使用内容的条件。

[0027] 根据本发明的另一个实施例，提供了一种信息处理设备，其可连接到结合有存储介质的存储设备并且其中保存了要记录到存储设备的内容。该信息处理设备包括 ：乱数生成请求部件，该乱数生成请求部件被配置为向存储设备发送乱数生成请求 ；乱数接收部件，该乱数接收部件被配置为响应于乱数生成请求被发送到存储设备，从存储设备接收构成乱数生成请求所特有的变量的乱数 ；加密部件，该加密部件被配置为利用从存储设备接收的乱数对关于内容的数据文件进行加密 ；数据记录部件，该数据记录部件被配置为将经加密的数据文件记录到存储设备的存储介质 ；散列计算部件，该散列计算部件被配置为计算经

加密的数据文件的散列值；以及乱数写入请求部件，该乱数写入请求部件被配置为向存储设备发送包括散列值的乱数写入请求。

[0028] 优选地，信息处理设备可以还包括：发送请求部件，该发送请求部件被配置为向存储设备发送请求从存储设备发送乱数和散列值的发送请求；管理信息接收部件，该管理信息接收部件被配置为响应于发送请求，从存储设备接收存储在存储介质中的乱数和散列值；数据获取部件，该数据获取部件被配置为从存储设备获取存储在存储介质中的经加密的数据文件；散列计算部件，该散列计算部件被配置为计算从存储设备获取的经加密的数据文件的散列值；散列值匹配部件，该散列值匹配部件被配置为将计算出的散列值与从存储设备接收的散列值相匹配；以及解密部件，该解密部件被配置为在两个散列值之间存在完全匹配的情况下利用从存储设备接收的乱数对经加密的数据文件进行解密。

[0029] 优选地，信息处理设备可以还包括：认证部件，该认证部件被配置为与存储设备执行相互认证以共享会话密钥；以及MAC值计算部件，该MAC值计算部件被配置为利用会话密钥计算散列值的MAC值。乱数写入请求部件可以向存储设备发送包括散列值和从散列值得出的MAC值的乱数写入请求。在计算散列值的MAC值时，MAC值计算部件可以优选地利用会话密钥计算组合的散列值和乱数的MAC值。

[0030] 优选地，存储设备的存储介质可以具有作为存储区域的普通数据存储区域和安全数据管理区域。经加密的数据文件可以被写入到普通数据存储区域，并且散列值和乱数可以被写入到数据管理区域。

[0031] 优选地，关于内容的数据文件可以包括由内容文件、内容密钥文件、标识信息文件和使用条件文件组成的四种文件中的至少一种，内容文件中具有内容，内容密钥文件被用于对经加密的数据文件进行解密，标识信息文件表示用于标识内容的标识信息，使用条件文件限定使用内容的条件。

[0032] 根据本发明的另一个实施例，提供了一种存储设备，其可连接到信息处理设备并且用于存储由信息处理设备保存的内容。该存储设备包括：乱数生成请求接收部件，该乱数生成请求接收部件被配置为接收来自信息处理设备的乱数生成请求；乱数生成部件，该乱数生成部件被配置为响应于接收到乱数生成请求，生成构成乱数生成请求所特有的变量的乱数；乱数发送部件，该乱数发送部件被配置为将乱数发送到信息处理设备；存储介质，该存储介质被配置为存储关于内容的数据文件，该数据文件被信息处理设备利用乱数进行了加密；乱数写入请求接收部件，该乱数写入请求接收部件被配置为接收来自信息处理设备的包括经加密的数据文件的散列值的乱数写入请求；以及乱数记录部件，该乱数记录部件被配置为响应于接收到乱数写入请求，在将乱数写入请求中包括的散列值和乱数生成部件生成的乱数记录到存储介质时，将散列值和乱数关联起来。

[0033] 优选地，存储设备可以还包括：发送请求接收部件，该发送请求接收部件被配置为从信息处理设备接收请求向信息处理设备发送存储在存储介质中的乱数和散列值的发送请求；以及管理信息发送部件，该管理信息发送部件被配置为响应于接收到发送请求，读出存储在存储介质中的乱数和散列值并向信息处理设备发送。

[0034] 优选地，存储设备可以还包括认证部件，该认证部件被配置为与信息处理设备执行相互认证以共享会话密钥。乱数写入请求接收部件可以接收包括散列值和由信息处理设备利用会话密钥计算出的散列值的MAC值的乱数写入请求。存储设备可以还包括验证部

件，该验证部件被配置为响应于接收到乱数写入请求，利用会话密钥计算乱数写入请求中包括的散列值的MAC值，以便验证在计算出的MAC值和乱数写入请求中包括的散列值的MAC值之间是否存在完全匹配。如果在两个MAC值之间存在完全匹配，则乱数记录部件可以在将散列值和乱数记录到存储介质时将散列值与乱数关联起来。

[0035] 优选地，在计算散列值的MAC值时，验证部件可以利用会话密钥计算组合的散列值和乱数的MAC值。

[0036] 优选地，存储设备的存储介质可以具有作为存储区域的普通数据存储区域和安全数据管理区域；其中经加密的数据文件可以被写入到普通数据存储区域，并且散列值和乱数可以被写入到数据管理区域。

[0037] 优选地，存储设备可以是可移除地附接到信息处理设备的可移除介质。

[0038] 优选地，存储设备可以是被构造成将存储介质与被配置为向存储介质写入数据和从存储介质读取数据的驱动器相集成的内容处理设备。

[0039] 优选地，关于内容的数据文件可以包括由内容文件、内容密钥文件、标识信息文件和使用条件文件组成的四种文件中的至少一种，内容文件中具有内容，内容密钥文件被用于对经加密的数据文件进行解密，标识信息文件表示用于标识内容的标识信息，使用条件文件限定使用内容的条件。

[0040] 根据本发明的另一个实施例，提供了一种用于结合信息处理设备使用的记录方法，该信息处理设备可连接到结合有存储介质的存储设备并且其中保存了要记录到存储设备的内容。该记录方法包括以下步骤：在向存储设备记录内容时，向存储设备发送乱数生成请求；响应于乱数生成请求被发送到存储设备，从存储设备接收构成乱数生成请求所特有的变量的乱数；利用从存储设备接收的乱数对关于内容的数据文件进行加密；将经加密的数据文件记录到存储设备的存储介质；计算经加密的数据文件的散列值；以及向存储设备发送包括散列值的乱数写入请求，从而使得存储设备在将散列值和乱数记录到存储介质时将散列值与乱数关联起来。

[0041] 根据本发明的另一个实施例，提供了一种用于结合存储设备使用的记录方法，该记录设备可连接到信息处理设备并且用于存储由信息处理设备保存的内容。该记录方法包括以下步骤：接收来自信息处理设备的乱数生成请求；响应于接收到乱数生成请求，生成构成乱数生成请求所特有的变量的乱数；将乱数发送到信息处理设备；向存储介质记录关于内容的数据文件，该数据文件被信息处理设备利用乱数进行了加密；接收来自信息处理设备的包括经加密的数据文件的散列值的乱数写入请求；以及响应于接收到乱数写入请求，在将乱数写入请求中包括的散列值和在乱数生成步骤中生成的乱数记录到存储介质时，将散列值和乱数关联起来。

[0042] 根据本发明的另一个实施例，提供了一种用于结合信息处理设备的计算机使用的程序，该信息处理设备可连接到结合有存储介质的存储设备并且其中保存了要记录到存储设备的内容。该程序使得计算机执行包括以下步骤的过程：在向存储设备记录内容时，向存储设备发送乱数生成请求；响应于乱数生成请求被发送到存储设备，从存储设备接收构成乱数生成请求所特有的变量的乱数；利用从存储设备接收的乱数对关于内容的数据文件进行加密；将经加密的数据文件记录到存储设备的存储介质；计算经加密的数据文件的散列值；以及向存储设备发送包括散列值的乱数写入请求，从而使得存储设备在将散列值和乱

数记录到存储介质时将散列值与乱数关联起来。

[0043] 根据本发明的另一个实施例，提供了一种用于结合存储设备的计算机使用的程序，该记录设备可连接到信息处理设备并且用于存储由信息处理设备保存的内容。该程序使得计算机执行包括以下步骤的过程：接收来自信息处理设备的乱数生成请求；响应于接收到乱数生成请求，生成构成乱数生成请求所特有的变量的乱数；将乱数发送到信息处理设备；向存储介质记录关于内容的数据文件，该数据文件被信息处理设备利用乱数进行了加密；接收来自信息处理设备的包括经加密的数据文件的散列值的乱数写入请求；以及响应于接收到乱数写入请求，在将乱数写入请求中包括的散列值和在乱数生成步骤中生成的乱数记录到存储介质时，将散列值和乱数关联起来。

[0044] 根据本发明的实施例，如上所述，可以安全地存储内容，而不会变得依赖于所使用的存储设备（即介质）的物理格式。

## 附图说明

[0045] 图 1 是示出在传统的 AACS 方案中内容如何被记录到光盘的序列图；

[0046] 图 2A 和 2B 是说明作为本发明第一实施例来实现的记录系统与使用传统光盘作为其存储介质的记录系统相比较的示意图；

[0047] 图 3 是示出作为第一实施例的一部分的主机设备的典型结构的框图；

[0048] 图 4 是示出作为第一实施例的一部分的可移除介质的典型结构的框图；

[0049] 图 5 是示出构成第一实施例的该主机设备和该可移除介质的功能结构的框图；

[0050] 图 6 是示出用于结合作为第一实施例的记录系统使用的记录方法的序列图；

[0051] 图 7 是图示出用于结合作为第一实施例的记录系统使用的内容使用方法的序列图；

[0052] 图 8 是说明作为本发明的第二实施例来实现的记录系统的示意图；

[0053] 图 9 是示出构成第二实施例的记录设备的便携式再现设备的典型结构的框图；以及

[0054] 图 10A、10B 和 10C 是说明本发明第一实施例利用的可移除介质上通常记录的文件的示意图。

## 具体实施方式

[0055] 现在将参考附图描述本发明的优选实施例。在附图和以下的描述中，就功能和结构而言相似或相对应的部件将利用相似的标号来指示，并且将省略对它们的冗余描述。

[0056] 以下首先通过参考图 2A 和 2B 来描述作为本发明的第一实施例来实现的记录系统 1。与图 2A 中的使用传统光盘作为其存储介质的记录系统相对照地，第一实施例的记录系统 1 在图 2B 中被示意性地概略示出。

[0057] 如图 2A 所示，传统的记录系统 3 具有主机设备 6，该主机设备 6 连接到光盘驱动器 7 或者结合了光盘驱动器 7。诸如蓝光光盘 (Blu-ray Disk，注册商标；以下称为 BD) 或 HD DVD 之类的充当存储介质的光盘 8 被加载到光盘驱动器 7 中。在记录系统 3 中，主机设备 6 可以利用驱动器 7 将内容、内容密钥等等的数据文件写入到光盘 8。在将内容等等记录到光盘 8 时，主机设备 6 和驱动器 7 按如图 1 所示的上述 AACS 方案在其间执行步骤。AACS

方案使得可以防止对内容进行非法拷贝或倒卷。例如，驱动器 7 生成绑定乱数并将所生成的绑定乱数写入到充当存储介质的光盘 8。

[0058] 与之不同的是，图 2B 所示的第一实施例的记录系统 1 由主机设备 10 和可移除地附接到主机设备 10 的可移除介质 20 构成。主机设备 10 和可移除介质 20 分别是信息处理设备和存储设备，两者都是根据本发明的实施例来实现的。可移除介质 20 是结合了诸如闪存之类的存储介质的存储设备；它可移除地附接到主机设备 10 的安装部件（例如插槽、连接器）。第一实施例的可移除介质 20 是将传统记录系统 3 的驱动器 7 与光盘 8 相集成的设备。这样，可移除介质 20 本身根据 AACS 规范生成绑定乱数并将其写入到存储介质。下文中将更详细地分别描述主机设备 10 和可移除介质 20。

[0059] 主机设备 10 是充当主机的记录设备，其使得诸如可移除介质 20 之类的存储设备（介质）记录内容、内容密钥等等的数据文件。通常，主机设备 10 由诸如个人计算机（简称为 PC) 之类的计算机装置（膝上型、桌面型或任何其他类型）构成。或者，主机设备 10 可以是 PDA（个人数字助理）、家庭视频游戏机、诸如 DVD/HDD 记录器之类的记录 / 再现设备、家庭信息装置或者某种其他适当的用户终端。

[0060] 可移除介质 20 是结合了能够容纳内容、内容密钥等等的数据文件的存储介质的存储设备。可移除介质 20 中结合的存储介质可以由闪存或由非易失性存储器等等组成的某种其他适当的半导体存储器构成。通常，可移除介质 20 可以是存储卡或者配备有连接器的存储器。存储卡是容纳在卡状封装中的诸如闪存之类的存储介质。存储卡已经被普遍用作诸如 PC、数码相机和便携式视频 / 音频播放器之类的数字数据装置的存储设备。配备有连接器的存储器基本上是这样一种封装，其包含闪存之类的存储介质，并且装备有用于插入到诸如 PC 之类的信息处理设备中的连接器。配备有连接器的存储器的代表是 USB（通用串行总线）存储器，其由装备有 USB 连接器的封装的闪存构成。

[0061] 可移除介质 20 可移除地连接到主机设备 10 的安装部件（例如插槽、连接器）。主机设备 10 可以向附接到安装部件的可移除介质 20 写入在内部保存的内容、内容密钥和其他数据的数据文件，并且可以从可移除介质 20 读取这种数据文件。

[0062] 第一实施例可以处理各种内容。内容例如可以包括：音频内容，比如音乐作品、讲座和无线电节目；视频内容，比如电影、TV 节目、视频节目和构成照片、绘画、示图等等的静止图像；电子书 (E-book)、视频游戏、和软件程序。虽然接下来的描述将集中于以音乐或视频内容来作为所关注的内容，但是它们只是用于描述目的，而不是要限制本发明的实施例。第一实施例将要处理的内容受到诸如 AACS 之类的各种方案下的著作权管理。

[0063] 以下参考图 3 描述的是充当第一实施例的信息处理设备的主机设备 10 的典型硬件构造。图 3 是示出作为第一实施例的一部分的主机设备 10 的典型结构的框图。在图 3 的示例中，主机设备 10 是 PC。或者，主机设备 10 可以是某种其他适当的信息处理设备。

[0064] 如图 3 所示，主机设备 10 例如由以下部分构成：CPU（中央处理单元）101、ROM（只读存储器）102、RAM（随机访问存储器）103、主机总线 104、桥接器 105、外部总线 106、接口 107、输入装置 108、输出装置 109、存储装置（例如 HDD) 110、插槽 111、驱动器 112、连接端口 113 和通信装置 114。

[0065] CPU101 充当算术处理单元和控制器，并且根据各种程序进行动作，以控制主机设备 10 的内部组件。CPU101 按照 ROM102 中保存的或者从存储装置 110 加载到 ROM102 中的

程序来执行各种处理。ROM102 容纳要被 CPU101 使用的程序和操作参数，并且还充当对从 CPU101 到存储装置 110 的访问操作进行缓冲的缓冲器。RAM103 临时容纳被 CPU101 用于处理的程序以及在 CPU101 的处理期间可能变化的参数。这些组件经由通常由 CPU 总线构成的主机总线 104 互连。主机总线 104 通过桥接器 105 连接到诸如 PCI（外围组件互连 / 接口）总线之类的外部总线 106。

[0066] 输入装置 108 一般由操作部件和输入控制电路构成，该操作部件通常由鼠标、键盘、触摸敏感型面板、按钮、开关和 / 或控制杆构成，该输入控制电路生成用于输出到 CPU101 的输入信号。主机设备 10 的用户可以对输入装置 108 进行操作以向主机设备 10 输入各种数据或者向主机设备 10 给出各种指令以便处理。输出装置 109 例如由显示装置和音频输出装置构成，该显示装置由 CRT（阴极射线管）显示单元、液晶显示器 (LCD) 单元或灯构成，该音频输出装置例如是扬声器。

[0067] 存储装置 110 是作为第一实施例的一部分的主机设备 10 的数据存储部件。这样，存储装置 110 通常可以由硬盘驱动器 (HDD) 组成。由充当存储介质的硬盘和驱动该硬盘的驱动器形成的存储装置 110 容纳要被要被 CPU101 执行的程序和操作的各种数据。

[0068] 插槽 111 是典型的安装装置，可移除介质 20 通过它被可移除地附接到主机设备 10。当诸如上述存储卡之类的可移除介质 20 被附接到插槽 111 时，主机设备 10 可以与可移除介质 20 进行数据通信。

[0069] 驱动器 112 是驱动可移除介质 20 的装置，它被结合在主机设备 10 中或者在外部附接到主机设备 10。驱动器 112 用于向插入在主机设备 10 的插槽 111 中的可移除介质 20 写入数据或从中读取数据。

[0070] 用于连接外部外围装置的连接端口 113 通常包括 USB 或 IEEE1394 连接器或其他适当的连接端子。连接端口 113 通过接口 107、外部总线 106、桥接器 105 和主机总线 104 连接到 CPU101 和其他组件。例如，诸如上述 USB 存储器之类的配备有连接器的可移除介质 20 可以连接到连接端口 111（例如连接到 USB 端口）。除了可移除介质 20 之外，诸如便携式视频 / 音频播放器、PDA 或 HDD 之类的外部设备通常也可利用线缆连接到连接端口 111。这些外部附件中的任何一个都可以充当根据本发明实施例的存储装置（下文中将参考图 8 和 9 对此进行论述）。

[0071] 通信装置 114 构成通信接口，该通信接口通常由用于连接到诸如因特网或 LAN 之类的网络 5 的通信装置组成。通信装置 114 向经由网络 5 连接的外部设备发送数据并从其接收数据。例如，通信装置 114 可以从网络 5 上的内容递送服务器接收内容、内容密钥、许可证和秘密密钥 (secretkey)。通信装置 114 可以令外部设备以有线方式或者通过无线 LAN 等等以无线方式连接到主机设备 10。

[0072] 以下参考图 4 描述的是充当第一实施例的存储设备的可移除介质 20 的硬件构造。图 4 是示出作为第一实施例的一部分的可移除介质 20 的典型结构的框图。

[0073] 如图 4 所示，可移除介质 20 由以下部分构成：闪存 21、通信装置 24、认证装置 25、乱数生成装置 26 和验证装置 27，它们都被包含在单个封装中。可移除介质 20 被指派以一介质 ID，该介质 ID 构成该介质所特有的标识信息。介质 ID 被安全地存储在闪存 21 中。

[0074] 闪存 21 是保存各种数据并被结合在可移除介质 20 中的典型存储介质。使闪存 21 被容纳在封装中构成了充当第一实施例的可移除介质 20 的存储卡。可移除介质 20 的闪存

21 可以被替换为其他适当的存储介质，其中包括非易失性存储器，比如 EEPROM（电可擦除可编程 ROM）、FeRAM（铁电 RAM）和 MRAM（磁阻 RAM）；或者被替换为某种其他适当的半导体存储器。

[0075] 闪存 21 被划分成多个存储区域。如图 4 所示，作为存储区域，闪存 21 具有普通数据存储区域 22 和安全数据管理区域 23。普通数据存储区域 22 是向其写入诸如内容、内容密钥、许可证（即内容使用条件信息）和内容属性信息之类的普通数据的区域。用户可以使主机设备 10 向普通数据存储区域 22 写入所需数据或从中读取所需数据。

[0076] 数据管理区域 23 是这样一个区域，其安全地存储管理信息，用于防止对普通数据存储区域 22 中的内容的非法使用，以便进行著作权保护。数据管理区域 23 充当用户对其的自由访问受到限制的秘密区域。在数据管理区域 23 中，每次数据文件被写入到普通数据存储区域 22 时生成的绑定乱数与所述数据文件的散列值或“内容令牌”(content token) 相关联地被记录。在图 4 的示例中，记录在普通数据存储区域 22 中的内容 #1 至 #n（未示出）分别与绑定乱数 #1 至 #n 和内容令牌 #1 至 #n 相关联。

[0077] 接下来是对绑定乱数（适当时简称为 BN）和内容令牌（适当时简称为 CT）的描述。

[0078] 根据上述 AACS 规范，当内容相关数据（包括内容本身、内容密钥、内容标识信息和许可证）的文件可被写入到一介质时，介质方重新生成绑定乱数并且使得所述数据文件与所生成的 BN 相关联的被记录到介质。每次内容相关数据文件被写入到介质时，BN 就以所述文件所特有的方式被生成并与该文件相关联地被记录。每当任何所记录的内容被更新时，新的 BN 就被生成，使得所关注的内容被新的 BN 绑定到所使用的介质。这种布置旨在防止对内容的非法倒卷。通常，BN 用于防止对关于内容使用的信息（即由许可证授权的拷贝次数、再现次数和再现时间限制）的违法初始化。

[0079] 在第一实施例的记录系统 1 中，由 AACS 定义的绑定乱数方案被用于防止对内容的非法倒卷。乱数是以记录到介质的每个内容文件所特有的方式生成的变量。诸如单次使用随机数或计数器值之类的任何值都可用作乱数，只要该数字的唯一性得到了确保即可。例如，第一实施例的记录系统 1 利用单次使用随机数来作为乱数，以便将内容“绑定性地”记录到介质。在这个意义上，第一实施例的乱数对应于 AACS 定义的绑定乱数（简称为 BN）。

[0080] 内容令牌 (CT) 是用于记录到介质的内容相关数据文件的散列值。内容相关数据文件例如可以包括内容本身的文件（例如视频内容数据文件、音频内容数据文件）、用于对经加密的内容进行解密的内容密钥的文件、内容标识信息（例如内容 ID、内容标题）和指定内容使用条件的许可证的文件。这种内容相关数据文件被写入到上述可移除介质 20 的闪存 21 中的普通数据存储区域 22。

[0081] 作为用于每个这种内容相关数据文件的散列值的 CT 构成与数据文件一一对应的标识信息。CT 代表相应的数据文件（即，作为令牌），并且允许记录在介质上的文件中的内容被唯一地标识。

[0082] 下面说明记录 CT 的意义。根据 AACS 的 BD 在传统上是与相应的内容相关数据文件一起同时被记录到同一扇区的，从而 BD 保持与所述文件相关联（参见图 1）。同时，第一实施例的记录系统 1 具有建立在存储设备的存储介质上（即，可移除介质 20 的闪存 21 中）的普通数据存储区域 22 和安全数据管理区域 23，如图 4 所示。内容相关数据文件被写入到普通数据存储区域 22，同时 BN 被记录到数据管理区域 23。CT 也与 BN 相关联地被写入到数

据管理区域 23。在这样被记录后，CT 允许了内容相关数据文件保持与存放在单独建立的存储区域中的 BN 相关联。这个特征提高了在记录 BN 和内容相关数据文件时的自由度，它可以被应用到按文件访问的可移除介质 20。

[0083] 下面参考图 4 描述的是可移除介质 20 的典型结构。通信装置 24 充当用于与主机设备 10 进行数据通信的通信接口。例如，通信装置 24 可以从主机设备 10 接收要记录的内容的数据文件、认证信息、CT、各种命令、递送的内容、内容密钥、许可证和秘密密钥。通过通信装置 24，主机设备 10 可以向附接到主机设备 10 的可移除介质 20 发送各种数据并从其接收各种数据。通常，主机设备 10 可以通过通信装置 24 将内容文件写入到闪存 21 或从其读取内容。

[0084] 认证装置 25 允许了主机设备 10 和可移除介质 20 之间的相互认证，并且允许了它们之间共享会话密钥。例如，认证装置 25 根据 AACS 执行其认证处理。

[0085] 乱数生成装置 26 生成上述的绑定乱数 (BN)。乱数生成装置 26 通常由生成单次使用随机数的随机数生成器或生成计数器值的计数器组成。每次通过通信装置 24 从主机设备 10 接收到乱数生成请求时，乱数生成装置 26 就生成单次使用随机数并将随机生成的数据作为 BN 返回给主机设备 10。

[0086] 验证装置 27 能够验证可移除介质 20 中记录的任何数据是否已被伪造或破坏。在记录系统 1 中，在主机设备 10 和可移除介质 20 之间交换的数据（例如 BN、CT）被补充以指派给所述数据以便防止数据伪造和毁坏的 MAC（消息认证代码）值。在接收到来自主机设备 10 的数据后，验证装置 27 计算接收到的数据的 MAC 值，并且将计算出的 MAC 值与主机设备 10 早先附加到所述数据的 MAC 值相比较，以便验证数据是否已被伪造或破坏。在将数据从可移除介质 20 发送到主机设备 10 时，验证装置 27 计算传出的数据的 MAC 值并且将计算出的 MAC 值附加到该数据。验证装置 27 从而用于确保主机设备 10 和可移除介质 20 之间的安全数据交换。

[0087] 以下参考图 5 描述的是第一实施例的主机设备 10 和可移除介质 20 就功能而言是如何构成的。图 5 是示出构成第一实施例的主机设备 10 和可移除介质 20 的功能结构的框图。

[0088] 如图 5 所示，主机设备 10 包括认证部件 122、乱数生成请求部件 124、乱数接收部件 126、验证部件 128、加密部件 130、内容数据库 132、数据记录部件 134、散列计算部件 136、MAC 值计算部件 138、乱数写入请求部件 140、发送请求部件 142、管理信息接收部件 144、验证部件 146、数据获取部件 148、散列计算部件 150、散列值匹配部件 152 和解密部件 154。这些组成部件可以通过将软件（例如有关功能执行程序）与硬件（例如 CPU101）相组合来实现，其中程序被安装在主机设备 10 中。或者，组成部件可以利用专用硬件来实现。

[0089] 可移除介质 20 包括认证部件 202、乱数生成请求接收部件 204、乱数生成部件 206、MAC 值计算部件 208、乱数发送部件 210、乱数写入请求接收部件 212、验证部件 214、乱数记录部件 216、发送请求接收部件 218、MAC 值计算部件 220 和管理信息发送部件 222。认证部件 202 由上述的认证装置 25（参见图 4）形成。乱数生成请求接收部件 204、乱数发送部件 210、乱数写入请求接收部件 212、发送请求接收部件 218 和管理信息发送部件 222 由通信装置 24 构成（图 4）。乱数生成部件 206 由乱数生成装置 26（图 4）形成。MAC 值计算部件 208、MAC 值计算部件 220 和验证部件 214 被包括在验证部件 27（图 4）中。乱数记录部

件 216 由用于根据来自主机设备 10 的指令向闪存 21 写入数据和从闪存 21 读取数据的装置（未示出）实现。

[0090] 接下来是对主机设备 10 和可移除介质 20 如何构成以及它们的组成部件如何与彼此相关的描述。

[0091] 当主机设备 10 要向可移除介质 20 写入数据或从可移除介质 20 读取数据时，主机设备 10 的认证部件 122 和可移除介质 20 的认证部件 202 利用 AACS 定义的方法来执行相互认证 (AACS-auth)，以便在它们之间共享会话密钥 Ks。认证部件 122 将会话密钥 Ks 转发到验证部件 128 和 146 以及 MAC 值计算部件 138（下文论述）。认证部件 202 将会话密钥 Ks 发送到验证部件 214 以及 MAC 值计算部件 208 和 220（下文论述）。在认证时，认证部件 202 从可移除介质 20 读取介质 ID 并且将所取回的介质 ID 发送到主机设备 10。

[0092] 当使主机设备 10 将保存在其中的内容写入到可移除介质 20 时，用户向主机设备 10 输入用于将所述内容记录到 20 的内容写入指令。响应于写入指令，主机设备 10 的乱数生成请求部件 124 向可移除介质 20 发送乱数生成请求（即用于请求乱数生成的命令），以提示后者生成 BN。

[0093] 来自主机设备 10 的乱数生成请求被可移除介质 20 的乱数生成请求接收部件 204 所接收。在接收到乱数生成请求后，乱数生成部件 206 生成作为每个乱数生成请求所特有的变量的乱数 (BN)。BN 通常可以是单次使用随机数或者某个其他适当的被确保了其唯一性的值。利用从认证部件 202 接收的会话密钥 Ks，MAC 值计算部件 208 计算由乱数生成部件 206 生成的 BN 的 MAC 值 (Dm)。乱数发送部件 210 向主机设备 10 发送由乱数生成部件 206 生成的 BN 和由 MAC 值计算部件 208 计算出的关于该 BN 的 MAC 值 (Dm)。

[0094] 主机设备 10 的乱数接收部件 126 接收来自可移除介质 20 的 BN 和 MAC 值 (Dm)。利用从认证部件 122 接收的会话密钥 Ks，验证部件 128 计算接收到的 BN 的 MAC 值。验证部件 128 进而将计算出的 MAC 值与接收到的 MAC 值 (Dm) 相比较。如果两个 MAC 值之间存在完全匹配，则接收到的 BN 被认为是合法的。如果两个 MAC 值之间存在不匹配，则 BN 可能已被伪造。在后一种情况下，记录处理被终止。

[0095] 主机设备 10 具有例如在存储装置 110 中建立的内容数据库 132。一个或多个内容相关数据文件（即内容本身、内容密钥等等的文件）被保存在内容数据库 132 中。如果验证部件 128 发现 BN 是正常的，则加密部件 130 从内容数据库 132 读取要记录的目标内容相关数据文件，例如要记录的内容的内容密钥文件 (Kt)。加密部件 130 进而根据预定的加密技术例如利用介质 ID、秘密密钥和 BN 来对所取回的内容密钥文件进行加密。

[0096] 数据记录部件 134 将被加密部件 130 加密的内容密钥文件 (EncKt) 写入到可移除介质 20 中的闪存 21 的普通数据存储区域 22。附接到主机设备 10 的可移除介质 20 充当主机设备 10 的外部存储设备。因此，主机设备 10 的数据记录部件 134 可以将诸如经加密的内容密钥文件 (EncKt) 之类的数据直接写入到可移除介质 20。或者，在记录内容密钥文件 (Kt) 时，数据记录部件 134 可以同时向可移除介质 20 写入与所述内容相关联的其他数据文件，例如内容本身的文件和指示有关许可证的文件。

[0097] 散列计算部件 136 利用预定的散列函数来计算经加密的内容密钥文件 (EncKt) 的散列值。散列值构成上述的内容令牌 (CT)。利用从认证部件 122 接收的会话密钥 Ks，MAC 值计算部件 138 计算由散列计算部件 136 生成的散列值 (CT) 的 MAC 值 (Dm2)。乱数写入请

求部件 140 向可移除介质 20 发送乱数写入请求，即请求记录可移除介质 20 生成的 BN 的命令。乱数写入请求包括由散列计算部件 136 生成的散列值 (CT) 和由 MAC 值计算部件 138 生成的从 CT 得出的 MAC 值 (Dm2)。

[0098] 乱数写入请求接收部件 212 从主机设备 10 接收包括 CT 和该 CT 的 MAC 值 (Dm2) 的乱数写入请求。验证部件 214 利用从认证部件 122 接收的会话密钥 Ks 来计算接收到的 CT 的 MAC 值。验证部件 214 进而将计算出的 MAC 值与接收到的 MAC 值 (Dm2) 相比较。如果两个 MAC 值之间存在完全匹配，则接收到的 CT 被认为是合法的。如果两个 MAC 值之间存在不匹配，则 CT 可能已被伪造。在后一种情况下，记录处理被终止。

[0099] 如果验证部件 214 发现 CT 是合法的，则乱数记录部件 216 将乱数生成部件 206 最近生成的乱数 (BN) 与从主机设备 10 接收的散列值 (CT) 关联起来，并且将 BN 和 CT 写入到闪存 21 的数据管理区域 23。

[0100] 当上述步骤已被执行时，要记录的目标内容相关数据文件被安全地写入到可移除介质 20 中的闪存 21。关于此记录处理的乱数 (BN) 和散列值 (CT) 也被安全地写入到闪存 21。

[0101] 当使得主机设备 10 使用可移除介质 20 上记录的内容时（例如再现、拷贝或移动），用户向主机设备 10 输入用于使用存在于可移除介质 20 上的所述内容的内容使用指令。响应于用户指令，主机设备 10 的发送请求部件 142 向可移除介质 20 发送请求可移除介质 20 发送存储在其上的乱数 (BN) 和散列值 (CT) 的发送请求（即，用于请求发送所述数据的命令）。此时，发送请求部件 142 请求可移除介质 20 发送与要使用的用户指定内容相关联的 BN 和 CT。对发送 BN 和 CT 的请求可以利用单个命令同时实现。或者，BN 的发送和 CT 的发送可以利用两个命令以时间上交错的方式来请求。

[0102] 可移除介质 20 的发送请求接收部件 218 接收到来自主机设备 10 的发送请求。响应于接收到的发送请求，MAC 值计算部件 220 从闪存 21 读取与指定的内容相关联的 BN 和 CT，并且利用从认证部件 202 接收的会话密钥 Ks 来计算 BN 的 MAC 值 (Dm3) 和 CT 的 MAC 值 (Dm4)。在接收到发送请求后，管理信息发送部件 222 从闪存 21 读取与指定的内容相关联的 BN 和 CT。管理信息发送部件 222 进而向主机设备 10 发送所取回的 BN 和 CT 以及由 MAC 值计算部件 220 生成的 BN 和 CT 的 MAC 值 (Dm3、DM4)。

[0103] 主机设备 10 的管理信息接收部件 144 接收来自可移除介质 20 的 BN、CT 和 MAC 值 (Dm3、Dm4)。验证部件 146 利用从认证部件 122 接收的会话密钥 Ks 来计算接收到的 BN 的 MAC 值和 CT 的 MAC 值。验证部件 146 进而将计算出的 BN 的 MAC 值与接收到的 MAC 值 (Dm3) 相比较。如果两个 MAC 值之间存在完全匹配，则接收到的 BN 被认为是合法的。在两个 MAC 值之间不匹配的情况下，BN 可能已被伪造。在这种情况下，正在进行的处理被终止。同样，验证部件 146 将计算出的 CT 的 MAC 值与接收到的 MAC 值 (Dm4) 相比较。如果两个 MAC 值之间存在完全匹配，则接收到的 CT 被认为是合法的。在两个 MAC 值之间不匹配的情况下，CT 可能已被伪造。在这种情况下，正在进行的处理也被结束。

[0104] 数据获取部件 148 从可移除介质 20 的闪存 21 获取关于要使用的内容的经加密的数据文件，例如经加密的内容密钥文件 (EncKt)。由于可移除介质 20 可以直接访问可移除介质 20，因此数据获取部件 148 可以从可移除介质 20 的闪存 21 读取有关数据文件。

[0105] 散列计算部件 150 计算由数据获取部件 148 获取的数据文件的散列值 (CT′)。

散列值匹配部件 152 将管理信息接收部件 144 接收的散列值 (CT) 与加密部件 130 计算出的散列值 (CT′ ) 相比较。在两个散列值 (CT、CT′ ) 之间不匹配的情况下,CT 可能已被伪造。在这种情况下,内容使用处理被终止。如果两个散列值之间存在完全匹配,则从可移除介质 20 接收的散列值 (CT) 被认为是合法的。

[0106] 当来自可移除介质 20 的散列值被认为是合法时,解密部件 154 对数据获取部件 148 获取的诸如经加密的内容密钥文件 (EncKt) 之类的经加密的数据文件进行解密,并且输出经解密的数据。例如,解密部件 154 利用管理信息接收部件 144 接收的 BN、介质 ID 和秘密密钥,根据预定的加密技术对内容密钥文件 (Kt) 进行解密。经解密的数据被提供给利用内容 ( 例如用于再现 ) 的内容使用部件 ( 未示出 )。解密部件 154 通过对经加密的内容密钥文件 (EncKt) 进行解密来获取作为经加密的数据的内容密钥文件 (Kt)。然后通过利用内容密钥文件对经加密的内容进行解密来对经加密的内容进行解密和再现。

[0107] 在记录内容相关数据文件时,如上所述,第一实施例的记录系统 1 利用可移除介质 20 发出的乱数 (BN) 来对数据文件进行加密。然后数据文件与 BN 和该数据文件的散列值 (CT) 相关联地被记录到可移除介质 20。BN 允许了数据文件被“绑定”到文件首次被记录到的可移除介质 20,从而防止了介质之间的内容的非法拷贝。在使用内容时,对从可移除介质 20 取回的有关数据文件的散列值 (CT′ ) 进行计算,并且将散列值 (CT′ ) 与从可移除介质 20 读取的 CT 相比较以寻找匹配。所比较的散列值之间的不匹配揭示了对所述数据文件的伪造 ( 例如,信息的违法初始化 )。这防止了对所述内容的非法使用。

[0108] 以下参考图 6 描述的是内容如何被第一实施例的记录系统 1 所记录。图 6 是示出用于结合第一实施例的记录系统使用的记录方法的序列图。

[0109] 在图 6 的步骤 S10 中,在向可移除介质 20 记录内容时,主机设备 10 与可移除介质 20 执行相互认证并与之共享会话密钥 Ks。在步骤 S12 中,以认证之后,主机设备 10 从可移除介质 20 获取唯一地指派给此介质 20 的介质 ID。作为此步骤的替换,可移除介质 20 可以计算介质 ID 的 MAC 值并将计算出的 MAC 值与介质 ID 一起发送给主机设备 10。这防止了对介质 ID 的伪造。

[0110] 在步骤 S14 中,主机设备 10 向可移除介质 20 发送乱数生成请求,以请求后者生成绑定乱数 (BN)。在步骤 S16 中,可移除介质 20 接收来自可移除介质 20 的乱数生成请求并且相应地生成诸如随机数或计数器值之类的 BN。BN 是特定于正在进行的记录处理的 ;一旦该处理被终止,同样的值就不会再次被生成。在步骤 S18 中,可移除介质 20 为对抗伪造计算 BN 的 MAC 值 (Dm)。在步骤 S20 中,可移除介质 20 将计算出的 MAC 值 (Dm) 与 BN 一起返回给主机设备 10。MAC 值是利用早先在步骤 S10 中共享的会话密钥 Ks,基于 AES( 高级加密标准 ),利用诸如 CBC-MAC( 密码区块链接 -MAC)、O-MAC 或 HMAC( 用于消息认证代码的密钥散列 ) 之类的函数来计算的。这同样适用于如下定义的 MAC 值的计算 :

[0111] Dm = MAC(Ks,绑定乱数 )

[0112] 在步骤 S22 中,主机设备 10 利用会话密钥 Ks 计算 BN 的 MAC 值 (Dm′ ),并且进行检查以判定从可移除介质 20 发送来的 MAC 值 (Dm) 是否与计算出的 MAC 值 (Dm′ ) 相匹配。如果两个 MAC 值之间存在完全匹配 (Dm′ = Dm),则意味着从可移除介质 20 获取的 BN 不是伪造的。在两个 MAC 值之间不匹配的情况下,BN 可能已被伪造。在后一情况下,不应当允许记录处理继续。所涉及的计算如下 :

[0113] Dm′ = MAC(Ks,绑定乱数)

[0114] 在步骤S24中,主机设备10利用从可移除介质20获取的BN来对关于要记录的内容的数据文件(例如内容密钥文件(Kt))进行加密。例如,主机设备10利用在步骤S12中获取的介质ID、在步骤S20中获得的BN和秘密密钥Km对内容密钥文件(Kt)进行加密。秘密密钥Km可以是根据某种其他适当的技术在多个主机设备10之间共享的一个(例如MKB)。作为加密技术,可以如下应用AACS可记录视频区块方案:

[0115] EncKt = AES-128E(Kpa,Kt xor AES-H(使用))

[0116] Kpa = AES-G(Km,绑定乱数)

[0117] 这里要加密的数据不限于内容密钥(Kt)。任何关于所关注的内容的数据都可以被加密,包括内容本身、限定内容的使用条件的许可证或者内容标识信息。

[0118] 在步骤S26中,主机设备10将经加密的数据文件写入到可移除介质20中的闪存21的普通数据存储区域22。如果对于要记录的数据存在多个内容密钥(Kt),则主机设备10可以将多个经加密的内容密钥(EncKt)放到单个内容密钥文件中(EncKt1...EncKtn)并将该内容密钥文件记录到可移除介质20。

[0119] 在步骤S28中,主机设备10计算经加密的内容密钥文件(EncKt1...EncKtn)的散列值,该散列值构成上述的内容令牌(CT)。计算散列值的方式可以是利用诸如SHA-1(安全散列算法1)之类的散列函数,或者通过采用其密钥基于主机设备10保存的秘密密钥的MAC值。所涉及的计算被定义如下:

[0120] 内容令牌= Hash(EncKt1‖...‖EncKtn)

[0121] 在步骤S30中,主机设备10利用会话密钥Ks计算从上述散列计算得出的CT的MAC值(Dm2)。虽然可以利用以下示出的表达式(1)来只获得CT的散列值Dm2,但是优选利用也在以下示出的表达式(2)来计算组合的CT和BN的MAC值Dm2。后一反映了BN和CT两者的MAC值(Dm2)允许了内容只与最近的BN相关联地被记录,从而防止了对内容相关信息的违法初始化,并且增强了安全性。所涉及的表达式如下:

[0122] Dm2 = MAC(Ks,内容令牌)...(1)

[0123] 或者

[0124] Dm2 = MAC(Ks,绑定乱数 ‖ 内容令牌)...(2)

[0125] 有了上述布置,当可移除介质20在相互认证之后共享会话密钥Ks时生成多个BN时,可以针对最近的BN来验证CT。验证在步骤S34中执行,这将在下文中描述。

[0126] 在步骤S32中,主机设备10向可移除介质20发送乱数写入请求,以请求后者记录所生成的BN。乱数写入请求包括以上在步骤S28中计算的CT和在步骤S30中生成的MAC值(Dm2)。

[0127] 在步骤S34中,可移除介质20接收来自主机设备10的乱数写入请求(CT和Dm2),并进而验证MAC值。更具体而言,利用会话密钥Ks,可移除介质20计算从主机设备10接收的CT的MAC值(Dm2′)(通过采用以下的表达式(3))或者计算组合的CT和BN的MAC值(Dm2′)(通过求助于以下的表达式(4))。可移除介质20随后将从主机设备10发送来的MAC值(Dm2)与计算出的MAC值(Dm2′)相比较以寻找匹配(Dm2′ = Dm2)。两个MAC值之间的完全匹配验证了从主机设备10获取的CT未被伪造。如果两个MAC值之间存在不匹配,则意味着CT已被伪造。于是记录处理应当被中断,并且内容密钥文件被从闪存21删

除。所涉及的表达式如下：

[0128] Dm2′ ＝ MAC(Ks,内容令牌)...(3)

[0129] 或者

[0130] Dm2′ ＝ MAC(Ks,绑定乱数 ‖ 内容令牌)...(4)

[0131] 如果在以上计算之后在两个 MAC 值 (Dm2、Dm2′ ) 之间检测到完全匹配，则可移除介质转到步骤 S36，并且将在步骤 S32 中从主机设备 10 接收的 CT 与早先在步骤 S16 中生成的 BN 相关联地记录到闪存 21 的数据管理区域 23。如果与 BN 相对应的 CT 已经被记录在闪存 21 中，则现有的 CT 不会被用新的覆写。这防止了对相同 BN 的重复登记。

[0132] 根据上述用于与第一实施例的记录系统结合使用的记录方法，可移除介质 20 在将诸如内容 (Kt) 之类的数据文件记录到可移除介质 20 时生成唯一的绑定乱数 (BN)。BN 被用于对数据文件 (Kt) 加密，并且经加密的数据文件 (EncKt) 与 BN 一对一地关联并被安全地记录。如果 BN 和数据文件是在没有被进一步处理的情况下被记录的，那么两者应当在其间没有关联的情况下被写入到闪存 21 中的两个不同的存储区域 22 和 23。利用第一实施例，作为数据文件的散列值的 CT 与 BN 相关联地被记录到数据管理区域 23。CT 充当代表数据文件本身的标识信息。因此，将 CT 与 BN 相关联地写入到数据管理区域 23 使得可以将记录在数据管理区域 23 中的 BN 与写入到普通数据存储区域 22 的数据文件关联起来。

[0133] 在以上上下文中，还可以通过将诸如内容密钥 (Kt) 之类的数据文件本身记录到数据管理区域 23 来将 BN 与数据文件关联起来。但是，可移除介质 20 上的安全数据管理区域 23 只具有有限的大小（例如几十千字节）。这需要将要记录的数据大小保持在预定限度之下。根据第一实施例，通过向数据管理区域 23 写入作为数据文件的散列值的 CT，可以减小数据管理区域 23 的数据大小。

[0134] 当 BN 和 CT 如上所述彼此关联地被记录到可移除介质 20 时，不需要像传统的记录方法（图 1）那样将诸如内容密钥 (Kt) 之类的数据文件和 BN 记录到同一扇区。因为数据文件和 BN 以时间上交错的方式被分开写入到不同的存储区域，因此在设计要记录的数据文件的文件格式方面提供了很高的自由度。

[0135] 当诸如内容密钥 (Kt) 之类的数据文件被加密时（在步骤 S24 中），介质 ID 和内容密钥 (Kt) 被秘密地与彼此关联起来。这意味着数据文件仅在被记录于具有所述介质 ID 的可移除介质 20 上的情况下才可使用。在以这种方式将数据文件“绑定”到可移除介质 20 的情况下，防止了介质间的数据文件的违法拷贝。

[0136] 当在以上步骤 S30 中计算 CT 的 MAC 值时，优选计算组合的 CT 和 BN 的 MAC 值 (Dm2)，以便计算出的 MAC 值 (Dm2) 将在步骤 S34 中被验证。计算 MAC 值的优选方式的原因在于可移除介质 20 生成的最近的 BN 可与 CT 相关联地被写入到可移除介质 20，MAC 值 (Dm2) 作为组合的 CT 和 BN 的 MAC 值 (Dm2) 被验证。在可移除介质 20 在与主机设备 10 共享单个会话密钥 Ks 期间生成多个 BN 的情况下（即，在内容被多次记录的情况下），这种布置是有效的。在这种情况下，如果先前生成的 BN 保持有效，则被从可移除介质 20 移出的内容能够利用旧的 BN 被写回到它。为了防止这种欺骗性作法，需要只使得可移除介质 20 生成的最近的 BN 有效，以便一次性使用。因而，优选地，在 BN 和 CT 被记录时，组合的 BN 和 CT 的 MAC 值 (Dm2) 被用于验证。

[0137] 以下参考图 7 描述的是内容如何被第一实施例的记录系统 1 使用。图 7 是图示出

用于结合作为第一实施例的记录系统 1 使用的内容使用方法的序列图。

[0138] 在图 7 的步骤 S50 中，在使用记录在可移除介质 20 上的内容时，主机设备 10 和可移除介质 20 执行相互认证以在其间共享会话密钥 Ks。在步骤 S52 中，在相互认证之后，主机设备 10 从可移除介质 20 获取唯一地指派给可移除介质 20 的介质 ID。此时，可移除介质 20 可以计算介质 ID 的 MAC 值并将计算出的 MAC 值与介质 ID 一起发送给主机设备 10。这防止了对介质 ID 的伪造。

[0139] 在步骤 S54 中，主机设备 10 向可移除介质 20 发送 BN 发送请求，以请求可移除介质 20 发送存储在其上的 BN。在接收到来自主机设备 10 的发送请求后，可移除介质 20 转到步骤 S56，并且从闪存 21 的数据管理区域 23 读取存储的 BN。此时，可移除介质 20 读取与主机设备 10 指定的内容相关联的 BN。虽然在图 7 中未示出，但主机设备 10 在使用内容时从可移除介质 20 获取存储的内容的列表并且显示该内容列表以供用户从中选择。当用户从显示的列表中选择所需的内容时，主机设备 10 将用户指定的内容指定为要使用的内容。主机设备 10 从而拥有了关于先前存储在可移除介质 20 上的内容的信息，并且相应地请求从可移除介质 20 发送与用户选择的内容相关联的 BN。

[0140] 在步骤 S58 中，利用在步骤 S50 中共享的会话密钥 Ks，可移除介质 20 计算从闪存 21 取回的 BN 的 MAC 值 (Dm3)。在步骤 S60 中，可移除介质 20 将计算出的 MAC 值 (Dm3) 与所述 BN 一起发送到主机设备 10。所涉及的计算被定义如下：

[0141] Dm3 = MAC(Ks,绑定乱数)

[0142] 在接收到来自可移除介质 20 的 BN 后，主机设备 10 转到步骤 S62，利用会话密钥 Ks 计算 BN 的 MAC 值 (Dm3′)，并且进行检查以了解从可移除介质 20 发送来的 MAC 值 (Dm3) 是否与计算出的 MAC 值 (Dm3′) 相匹配。两个 MAC 值之间的完全匹配验证了从可移除介质 20 获取的 BN 未被伪造。如果在两个 MAC 值 (Dm3、Dm3′) 之间存在不匹配，则意味着 BN 可能已被伪造。在后一种情况下，内容使用处理必须被中断。所涉及的计算被定义如下：

[0143] Dm3′ = MAC(Ks,绑定乱数)

[0144] 在步骤 S64 中，主机设备 10 向可移除介质 20 发送 CT 发送请求，以请求后者发送存储的 CT。在接收到来自主机设备 10 的发送请求后，可移除介质 20 转到步骤 S66 并且从闪存 21 的数据管理区域 23 读取有关 CT。此时，可移除介质 20 取回与主机设备 10 指定的内容相关联的 CT(即，与早先在步骤 S56 中读取的 BN 相关的 CT)。

[0145] 在步骤 S68 中，利用在步骤 S50 中共享的会话密钥 Ks，可移除介质 20 计算组合的 BN 和从闪存 21 取回的 CT 的 MAC 值 (Dm4)。在步骤 S70 中，可移除介质 20 将 CT 与计算出的 MAC 值 (Dm4) 一起返回给主机设备 10。所涉及的计算被定义如下：

[0146] Dm4 = MAC(Ks,绑定乱数 ‖ 内容令牌)

[0147] 在接收到来自可移除介质 20 的 CT 后，主机设备 10 转到步骤 S72，利用会话密钥 Ks 计算 BN 的 MAC 值 (Dm4′)，并且进行检查以判定从可移除介质 20 发送来的 MAC 值 (Dm4) 是否与计算出的 MAC 值 (Dm4′) 相匹配。两个 MAC 值之间的完全匹配验证了从可移除介质 20 获取的 CT 未被伪造。两个 MAC 值 (Dm4、Dm4′) 之间的不匹配表明 CT 可能已被伪造。在后一种情况下，内容使用处理必须被中断。所涉及的计算被定义如下：

[0148] Dm4′ = MAC(Ks,绑定乱数 ‖ 内容令牌)

[0149] 在步骤 S74 中，主机设备 10 从可移除介质 20 中的闪存 21 的普通数据存储区域 22

获取与要使用的内容相关联的数据文件。例如，数据文件可以是利用 BN 等等加密的内容密钥 (Kt) 文件、利用内容密钥 (Kt) 加密的内容文件，或者许可证。以下描述的是获取内容密钥文件 (Kt) 的示例。

[0150] 在步骤 S76 中，主机设备 10 计算从可移除介质 20 获得的内容密钥文件 (EncKt1...EncKtn) 的散列值 (CT′ )。该散列值被称为“内容令牌′ (CT′ )”。所涉及的计算被定义如下：

[0151] 内容令牌′ = Hash(EncKt1 ‖ ... ‖ EncKtn)

[0152] 在步骤 S78 中，主机设备 10 将在步骤 S76 中计算出的散列值 (CT′ ) 与早先在步骤 S70 中从可移除介质 20 接收的 CT 相比较，以了解两个散列值 (CT、CT′ ) 是否匹配。如果在两个散列值之间存在不匹配，则意味着从可移除介质 20 接收的 CT 可能已被伪造。在这种情况下，内容使用处理必须被中断。

[0153] 在两个散列值 (CT、CT′ ) 之间完全匹配的情况下，主机设备 10 转到步骤 S80，并利用从可移除介质 20 获得的 BN 来对经加密的内容密钥 (Kt) 的数据文件进行解密。例如，主机设备 10 利用在步骤 S52 中获得的介质 ID、在步骤 S60 中获取的 BN 和秘密密钥 Km 对内容密钥 (Kt) 进行解密。秘密密钥 Km 通常可以是利用某种适当的技术在多个主机设备 10 之间共享的一个 ( 例如 MKB)。与以上论述的加密方法一样，解密可以基于如下定义的 AACS 可记录视频区块方案来执行：

[0154] Kt = AES-128D(Kpa, EncKt)xor AES-H( 使用 )

[0155] Kpa = AES-G(Km, 绑定乱数 )

[0156] 如上所述获得内容密钥 (Kt) 的经解密的数据。经解密的内容密钥 (Kt) 随后被用来对存储在可移除介质 20 中的所关注的内容进行解密。更具体而言，主机设备 10 评估要使用的目标内容的许可证。如果符合许可证所提出的使用条件 ( 例如允许的再现次数、再现时间限制、拷贝次数等等)，则主机设备 10 从可移除介质 20 读取所关注的经加密的内容，并且利用经解密的内容密钥 (Kt) 对所取回的内容进行解密。主机设备 10 随后对经解密的内容进行解码，并且使得输出装置 109 输出所再现的数据的视频和音频。这样，主机设备 10 利用了存储在 ( 即，绑定到 ) 可移除介质 20 中的内容中的用户选择的内容。

[0157] 根据上述内容使用方法，主机设备 10 可以从可移除介质 20 安全地获取记录在可移除介质 20 上的 BN 和内容相关数据文件 ( 例如内容密钥文件 (Kt)) 的散列值 (CT)。主机设备 10 计算所获取的数据文件的散列值 (CT′ ) 并且将计算出的散列值 (CT′ ) 与被发现记录在可移除介质 20 上的散列值 (CT) 相比较以寻找匹配。这种比较揭示了可能在可移除介质 20 上实行的对数据文件的任何伪造或违法初始化。如果检测到这种伪造或违法初始化，则终止内容使用处理以便保护所涉及的著作权。

[0158] 以下参考图 8 和 9 描述的是作为本发明的第二实施例的记录系统 2。图 8 是说明作为本发明的第二实施例来实现的记录系统 2 的示意图。图 9 是示出构成第二实施例的记录设备的便携式再现设备 30 的典型结构的框图。

[0159] 联系以上论述的第一实施例，以存储卡为代表的可移除介质 20 被引用作为存储设备。可移除介质 20 被示为将诸如内容之类的数据存储到其存储介质上。应当注意，可移除介质 20 是不能够对存储在其中的内容进行再现的装置。与之不同的是，第二实施例的存储设备例如可以由这样一个内容处理设备构成，该内容处理设备被构造为将其存储介质与

配置为向存储介质写入数据和从中读取数据的驱动器相集成。这类内容处理设备是装备有配备了驱动器的存储介质并具有对存储介质上存储的内容进行处理（例如再现）的能力的电子装置。这种内容处理设备通常可以包括诸如便携式视频/音频播放器、PDA和移动电话之类的便携式终端，以及诸如数码相机、数字摄像机和HDD记录器之类的记录/再现设备。在接下来的描述中，便携式再现设备（即便携式视频/音频播放器）将作为典型的内容处理设备被说明。

[0160] 如图8所示，第二实施例的记录系统2由主机设备10（对应于信息处理设备）和可连接到主机设备10的便携式再现设备30构成。便携式再现设备30通过诸如USB线缆之类的线缆或者通过诸如无线LAN之类的无线通信网络连接到主机设备10。与上述可移除介质20一样，便携式再现设备30根据AACS规范生成BN并将所生成的BN和CT记录到存储介质。

[0161] 下面描述便携式再现设备30的典型结构。

[0162] 如图9所示，便携式再现设备30包括控制装置31、输入装置32、充当存储介质的硬盘33、通信装置34、认证装置35、乱数生成装置36、验证装置37、驱动器38、再现装置39、显示装置40和音频输出装置41。

[0163] 控制装置31通常由微控制器组成。根据安装在便携式再现设备30中的程序工作的控制装置31对便携式再现设备30的组成装置进行控制。输入装置32一般由诸如触摸敏感型面板、按钮、开关和/或控制杆之类的操作元件以及生成输入信号并将其输出到控制装置31的输入控制电路构成。通过适当地操作输入装置32，便携式再现设备30的用户可以将各种数据和操作指令输入到设备30。

[0164] 硬盘33是被便携式再现设备30用来容纳各种数据的存储介质。驱动器38是用于向硬盘33写入数据和从硬盘33读取数据的装置。硬盘33和驱动器38构成硬盘驱动器(HDD)。HDD预先被指派以一介质ID，作为其唯一的标识信息。介质ID被安全地存储在HDD上。与上述可移除介质20中的闪存21一样，硬盘33具有两个存储区域：用于存储内容相关数据文件的普通数据存储区域22，以及用于将BN与CT相关联地进行存储的数据管理区域23。

[0165] 就功能而言，通信装置34和认证装置35基本上分别类似于可移除介质20的通信装置24和认证装置25（参见图4）。同样地，乱数生成装置36和验证装置37基本上分别类似于可移除介质20的乱数生成装置26和验证装置27。因而将不进一步论述对这些组成装置的详细说明。

[0166] 再现装置39由利用内容密钥(Kt)对经加密的内容进行解密的解密装置以及用于对内容解码的解码器构成。再现装置39具有对保存在硬盘33上的内容进行再现的能力。再现装置39再现的内容的视频数据被显示在显示装置40上；所再现的内容的音频数据通过音频输出装置41被输出。

[0167] 具有上述结构的便携式再现设备30具有与图5所示的可移除介质20相同的组成部件。当便携式再现设备30连接到主机设备10时，主机设备10所保存的内容可被写入到硬盘33，并且存储在便携式再现设备30中的内容可被主机设备10所利用。主机设备10和便携式再现设备30之间的内容记录和使用序列与以上图6和7中示出的相同，因而将不被进一步论述。

[0168] 以上段落中描述了作为本发明的第一和第二实施例来实现的记录系统 1 和记录系统 2 的结构，以及结合记录系统 1 和 2 执行的内容记录和使用方法。根据本发明的实施例，主机设备 10 将内容写入到作为存储设备的可移除介质 20 或便携式再现设备 30（以下称为介质 20、30）以便以后使用。每次内容要被记录时，为所述内容唯一地生成的绑定乱数 (BN) 就被安全地发送到主机设备 10。主机设备 10 进而生成关于要记录的目标内容的数据文件的散列值 (CT)，并且将所生成的 CT 与 BN 相关联地写入到介质 20、30。这防止了对记录在介质 20、30 上的任何内容的非法拷贝或者对关于该内容的信息的违法初始化。

[0169] 根据本发明实施例的记录方法具有不依赖于关于要记录的内容的数据文件（例如内容本身和内容密钥 (Kt) 文件）的格式的优点。本发明的记录方法还以独立于介质 20、30 的记录格式的方式工作。

[0170] 过去，根据基于 AACS 的用于结合诸如 BD 之类的光盘使用的普通记录方法（参见图 1），主机设备在 BN 生成之前需要指定光盘上记录诸如内容密钥文件 (Kt) 之类的数据文件的地址。必须符合该要求，以将 BN 和数据文件两者同时记录到同一扇区。在这个意义上，普通的记录方法严重依赖于介质（例如光盘）的物理格式。由于数据文件记录处理受到这样的限制，因此普通的记录方法不适合于根据 PTP（图片传输协议）、MTP（媒体传输协议）等等按文件访问的介质。每当记录在介质上的数据文件被更新（改变或删除）时，与该数据文件相对应的 BN 则必须被删除。因而，必须不断地监视与 BN 相关联的数据文件的更新。

[0171] 与之不同的是，根据本发明的实施例的记录方法，给定数据文件的散列值 (CT) 被用于将该数据文件与相应的 BN 关联起来。这使得无需将数据文件和 BN 两者同时记录到同一地址；两者可以以时间上交错的方式被分开写入到存储介质的两个不同的区域 22 和 23。当这样增强了记录数据文件时的自由度时，本发明的记录方法就可以有利地结合按文件访问的介质使用。

[0172] 根据以上实施例，在请求为数据文件生成 BN 时，主机设备 10 不需要预先掌握向其记录数据文件的地址，而这在过去是必不可少的。也不必声明向介质同时记录 BN 和数据文件。因为省略了这种在先掌握和声明所涉及的处理，设备的结构得到了简化，并且处理负担得到了减轻。

[0173] 此外，在使用内容时，以上实施例基于相关数据文件的散列值 (CT) 来验证该数据文件是否被伪造。当记录在介质 20、30 上的数据文件已被更新时，不需要删除与该数据文件相对应的 BN。也就是说，不需要不断地监视与 BN 相关联的数据文件的任何更新。

[0174] 以上实施例允许了从介质 20、30 中临时腾开 (save) 内容。过去，给定的数据文件及其 BN 被整体记录在 BD 上。因此，无法临时单独腾开数据文件（即，临时从介质中删除数据文件，然后将同一数据文件写回其中）。与之不同的是，根据本发明的记录方法，BN 被记录在数据管理区域 23 中，并且被独立于数据文件地进行管理。这使得可以从普通存储区域中临时腾开数据文件，然后利用保存在管理区域 23 中的相应 BD 将数据文件写回其中以供再使用。

[0175] 根据本发明的记录方法，与过去不同，不需要在生成 BN 时预先掌握介质上向其写入数据文件的地址。这意味着本发明的记录方法可以与在介质 20、30 上记录数据文件的记录格式相独立地使用。这转化成了允许主机设备 10 的应用自由选择用于向介质记录数据文件的方法的优点。

[0176] 本发明的记录方法可以被灵活地应用到诸如以下情况：单个巨大文件被创建在介质 20、30 上，作为向其记录内容密钥文件和内容的虚拟文件系统，或者内容密钥文件和内容在被记录之前被压缩成单个文件。下面参考图 10A 至 10C 说明这些情况的示例。

[0177] 根据本发明的记录方法，内容密钥和内容数据文件可以按普通的目录结构被正常记录到可移除介质 20，如图 10A 所示。利用本发明的记录方法，各自由一组多个数据文件（例如内容密钥和内容）构成的盘镜像可以各自作为单个文件 201 被记录，如图 10B 所示。如图 10C 所示，还可以利用诸如 Zip 之类的适当的文件压缩格式将多组多个数据文件（例如内容密钥和内容）各自压缩成单个文件 301，或者利用诸如 TAR（磁带编档和检索格式）之类的适当的编档格式将这种数据文件布置成单个文件以便记录。

[0178] 根据以上实施例，如上所述，内容可以通过相对灵活的序列被安全地记录到按文件访问的介质 20、30。还可以在不依赖于将数据文件写入到介质所用的格式的情况下将内容安全地记录到介质。

[0179] 虽然以上参考附图进行的描述包含许多特征，但是它们不应当被解释为限制本发明实施例的范围，而只是提供对本发明的一些当前优选的实施例的例示。应当理解，在不脱离所附权利要求的精神或范围的情况下，可以进行改变和变化。

[0180] 例如，虽然主机设备 10 被示为使用内容密钥 (Kt) 的散列值来作为要记录到介质 20、30 的数据文件的散列值（即内容令牌），但这并不是对本发明的实施例的限制。或者，散列值可以是诸如内容本身、内容密钥、许可证、内容标识信息或前述各项中的任何或全部的组合之类的给定内容相关数据文件的散列值。

[0181] 本领域的技术人员应当理解，取决于设计要求和其他因素，可以进行各种修改、组合、子组合和变更，只要它们处于所附权利要求或其等同物的范围之内。

[0182] 本发明包含与 2007 年 10 月 2 日向日本专利局提交的日本专利申请 JP2007-258992 相关的主题，这里通过引用将该申请的全部内容并入。

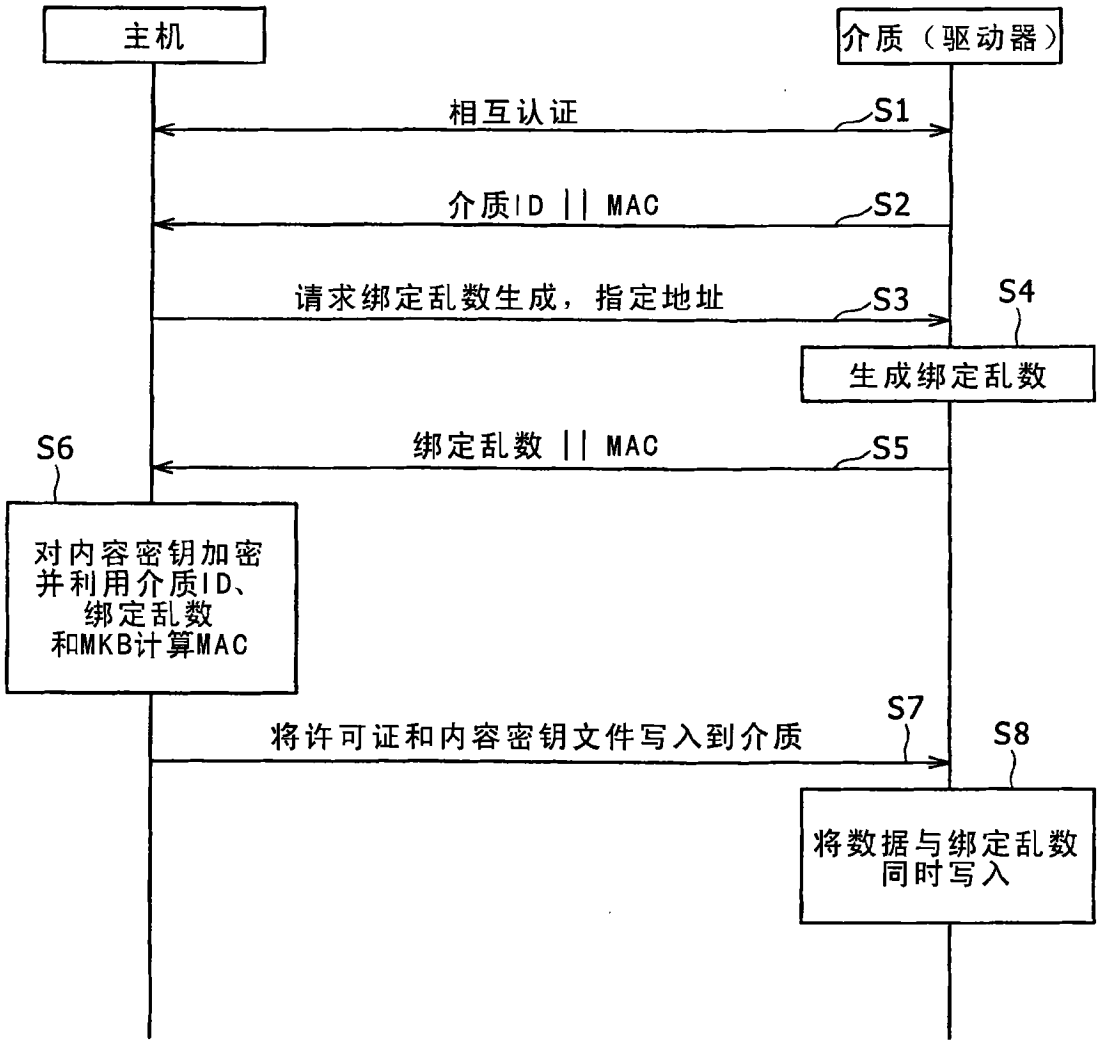
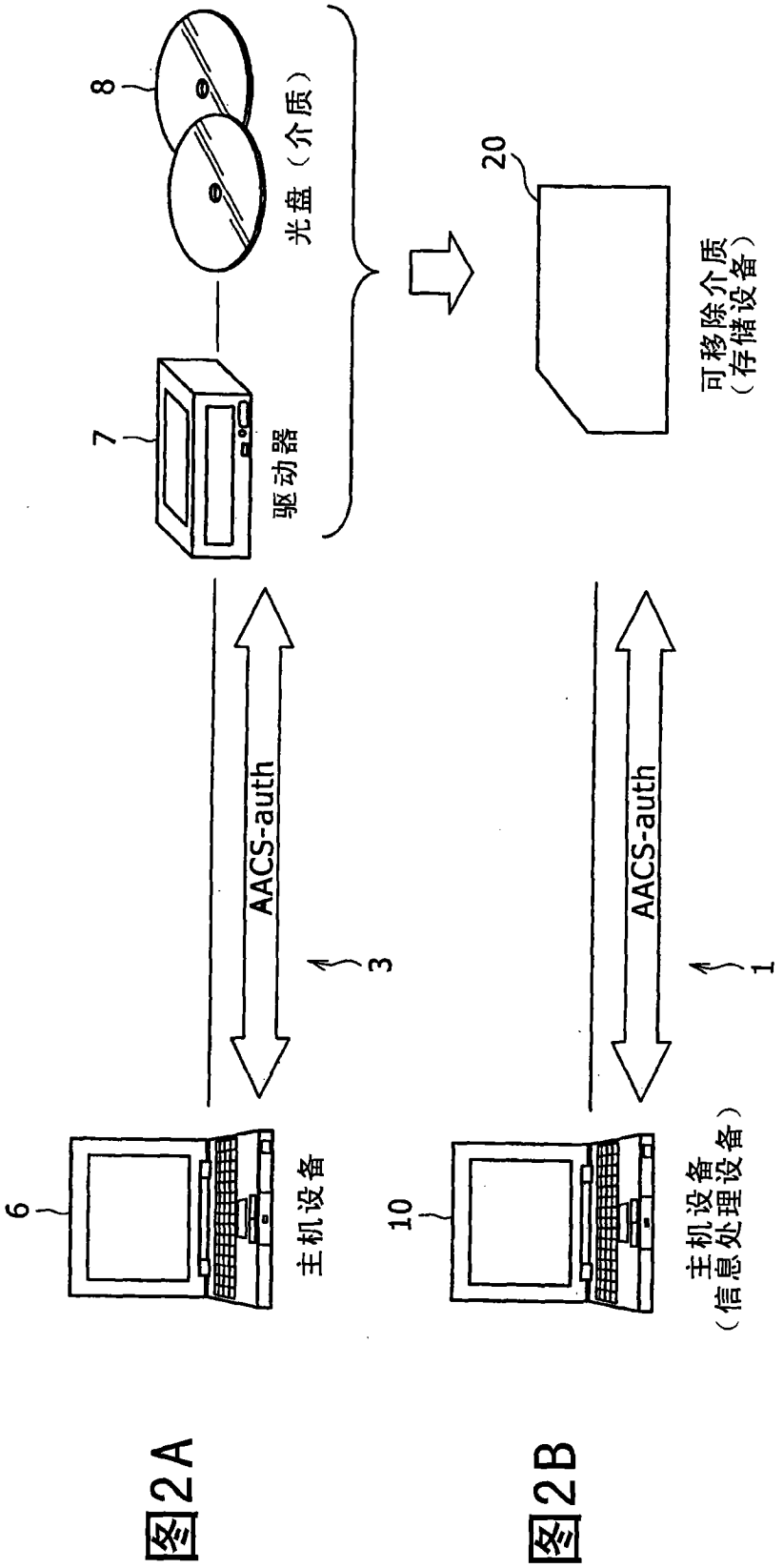

主机
介质（驱动器）
相互认证
S1
介质ID || MAC
S2
请求绑定乱数生成，指定地址
S3
S4
生成绑定乱数
S6
绑定乱数 || MAC
S5
对内容密钥加密
并利用介质ID、
绑定乱数
和MKB计算MAC
S7
将许可证和内容密钥文件写入到介质
S8
将数据与绑定乱数
同时写入

图 1


8
光盘（介质）
7
驱动器
6
主机设备
AACS-auth
3
1
图2A
20
可移除介质
（存储设备）
10
主机设备
（信息处理设备）
AACS-auth
1
图2B

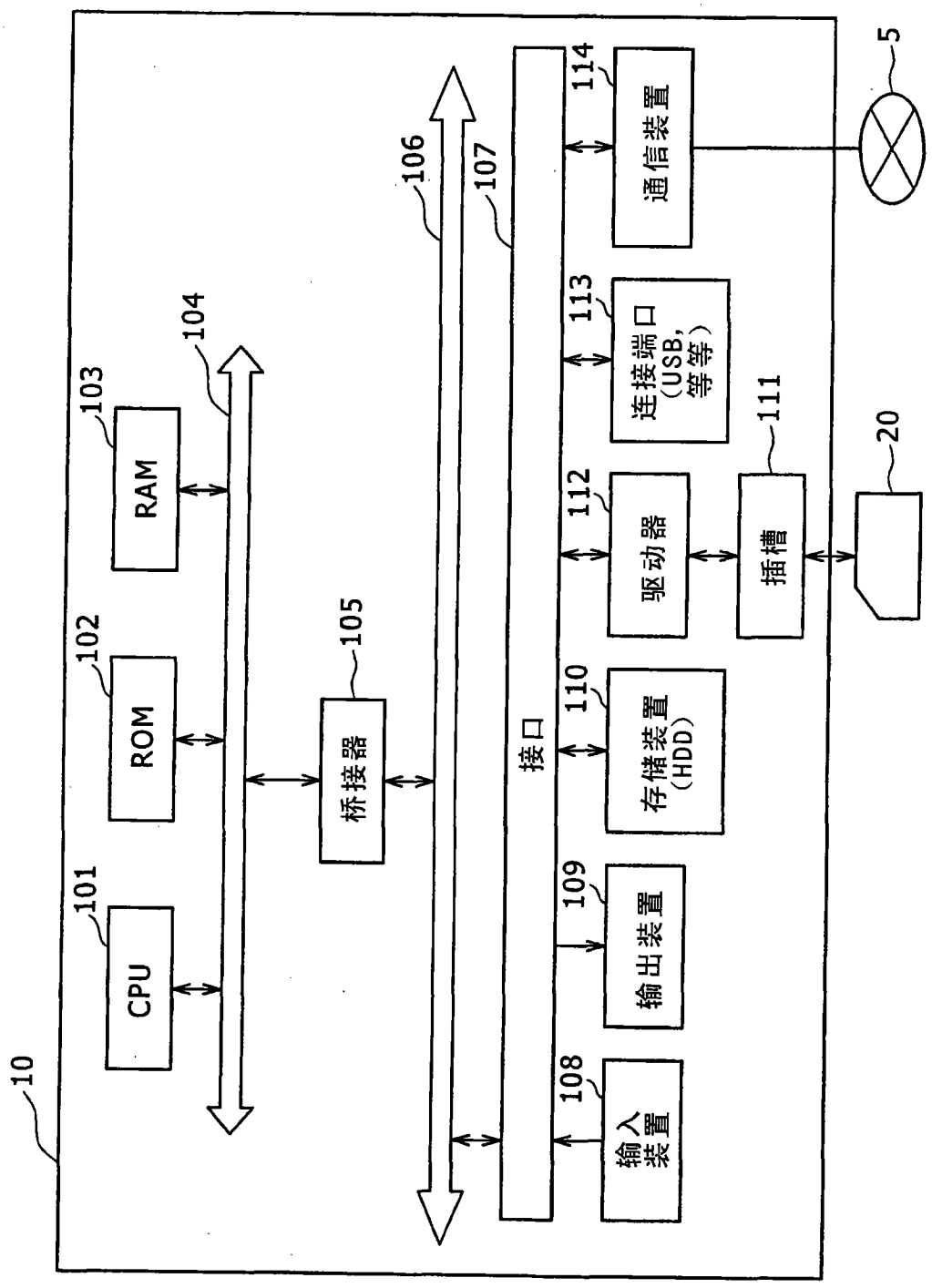

10
CPU
101
ROM
102
RAM
103
104
桥接器
105
106
107
接口
108
输入装置
109
输出装置
110
存储装置（HDD）
112
驱动器
111
插槽
20
113
连接端口（USB，等等）
114
通信装置
5

图3

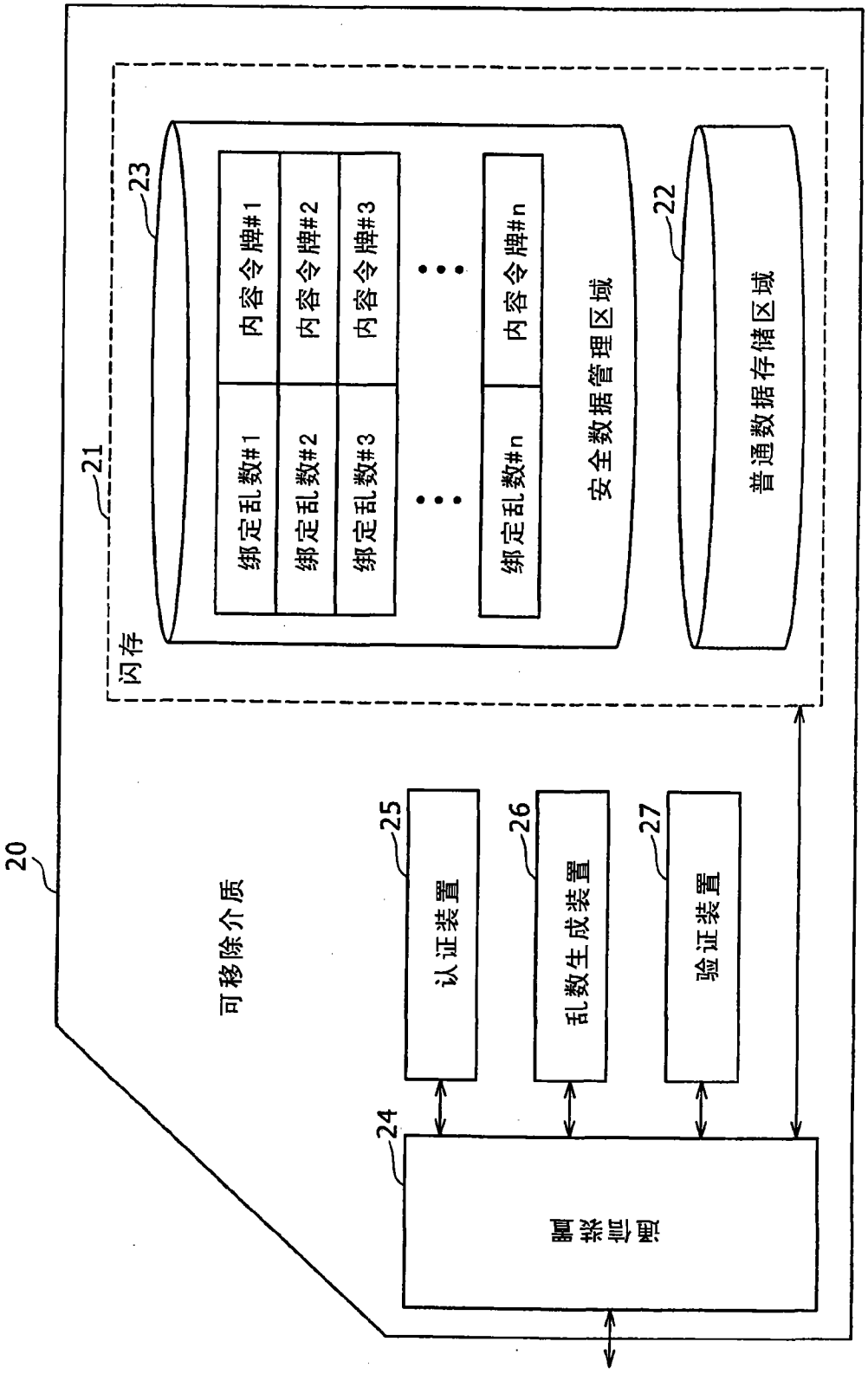

20
可移除介质
闪存
21
23
绑定乱数#1
绑定乱数#2
绑定乱数#3
绑定乱数#n
内容令牌#1
内容令牌#2
内容令牌#3
内容令牌#n
安全数据管理区域
22
普通数据存储区域
25
认证装置
26
乱数生成装置
27
验证装置
24
通讯装置

图4

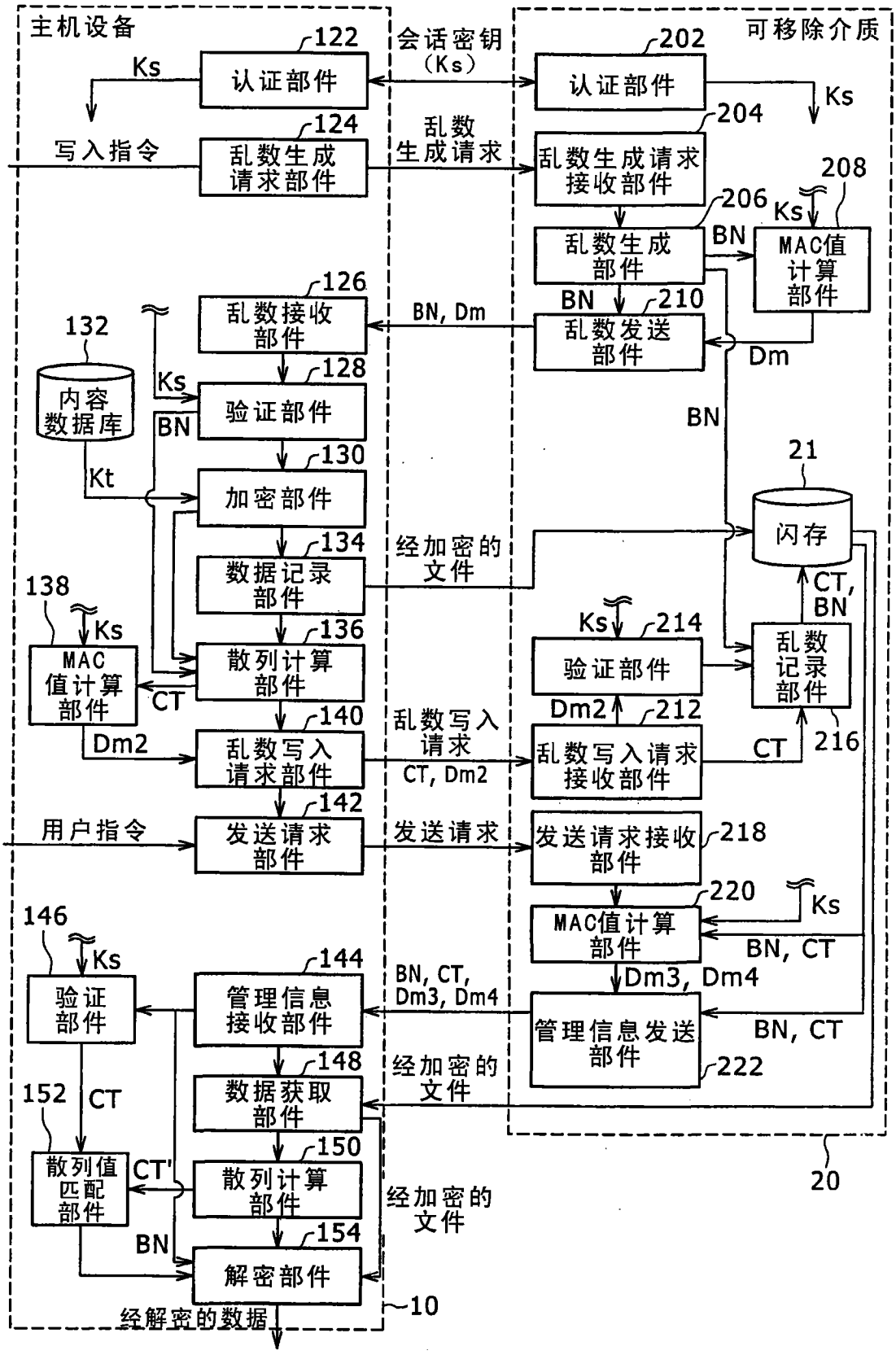

主机设备
可移除介质
会话密钥
(Ks)
认证部件
122
202
Ks
写入指令
乱数
生成请求
乱数生成
请求部件
124
乱数生成请求
接收部件
204
208
206
乱数生成
部件
MAC值
计算
部件
BN
BN, Dm
126
乱数接收
部件
乱数发送
部件
210
132
内容
数据库
128
验证部件
130
加密部件
Kt
Dm
BN
21
闪存
经加密的
文件
134
数据记录
部件
138
MAC
值计算
部件
136
散列计算
部件
CT
214
验证部件
乱数
记录
部件
CT,
BN
Dm2
212
216
140
乱数写入
请求部件
乱数写入
请求
CT, Dm2
乱数写入请求
接收部件
142
用户指令
发送请求
部件
发送请求
发送请求接收
部件
218
220
MAC值计算
部件
146
验证
部件
144
管理信息
接收部件
BN, CT,
Dm3, Dm4
Dm3, Dm4
管理信息发送
部件
222
148
数据获取
部件
152
CT
散列值
匹配
部件
CT'
150
散列计算
部件
154
解密部件
10
20
经解密的数据

图 5

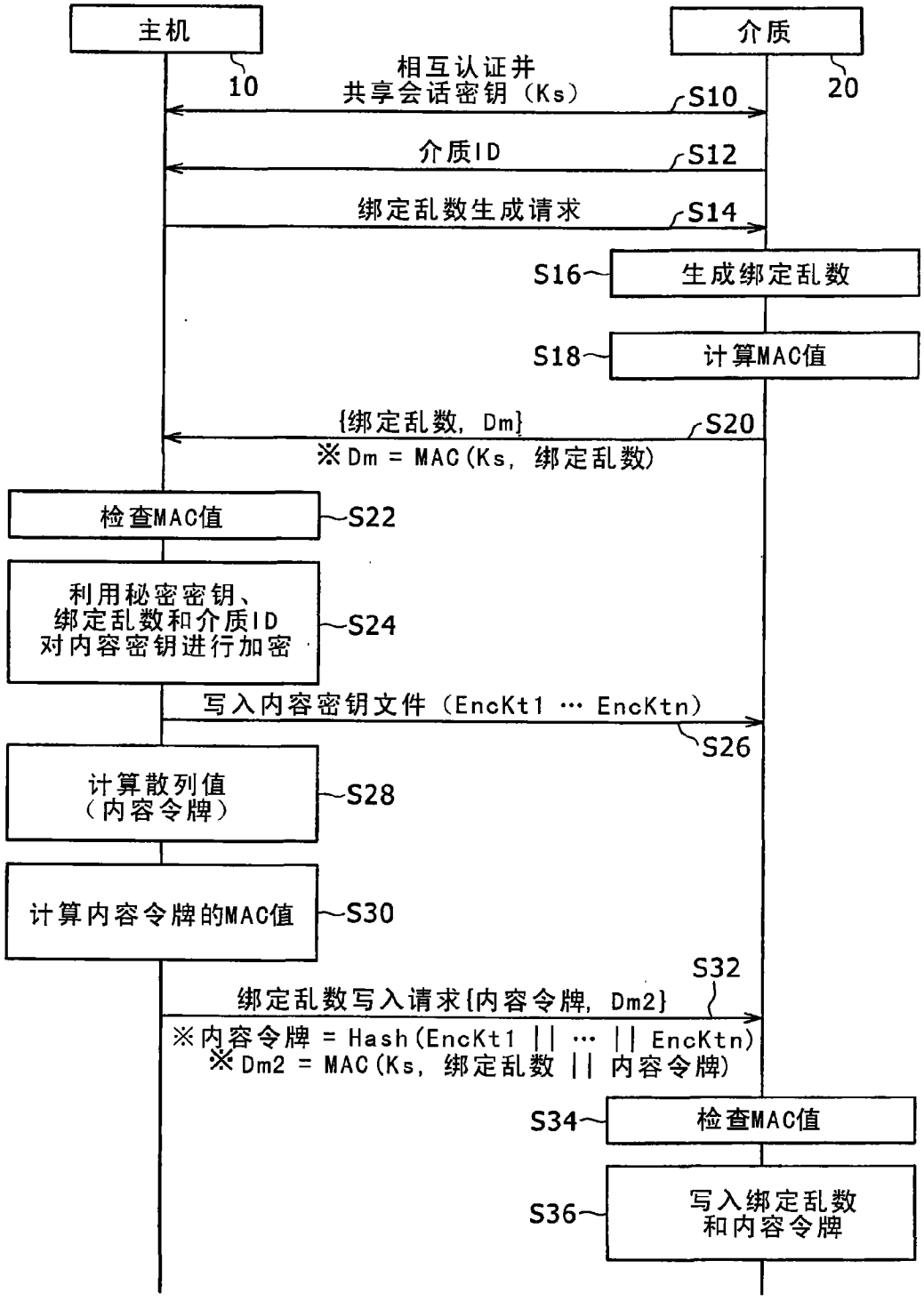

主机
介质
10
20
相互认证并
共享会话密钥（Ks）
S10
介质ID
S12
绑定乱数生成请求
S14
S16
生成绑定乱数
S18
计算MAC值
{绑定乱数，Dm}
S20
※Dm = MAC(Ks，绑定乱数)
检查MAC值
S22
利用秘密密钥、
绑定乱数和介质ID
对内容密钥进行加密
S24
写入内容密钥文件（EncKt1 … EncKtn）
S26
计算散列值
（内容令牌）
S28
计算内容令牌的MAC值
S30
S32
绑定乱数写入请求{内容令牌，Dm2}
※内容令牌 = Hash(EncKt1 || … || EncKtn)
※Dm2 = MAC(Ks，绑定乱数 || 内容令牌)
S34
检查MAC值
S36
写入绑定乱数
和内容令牌

图 6

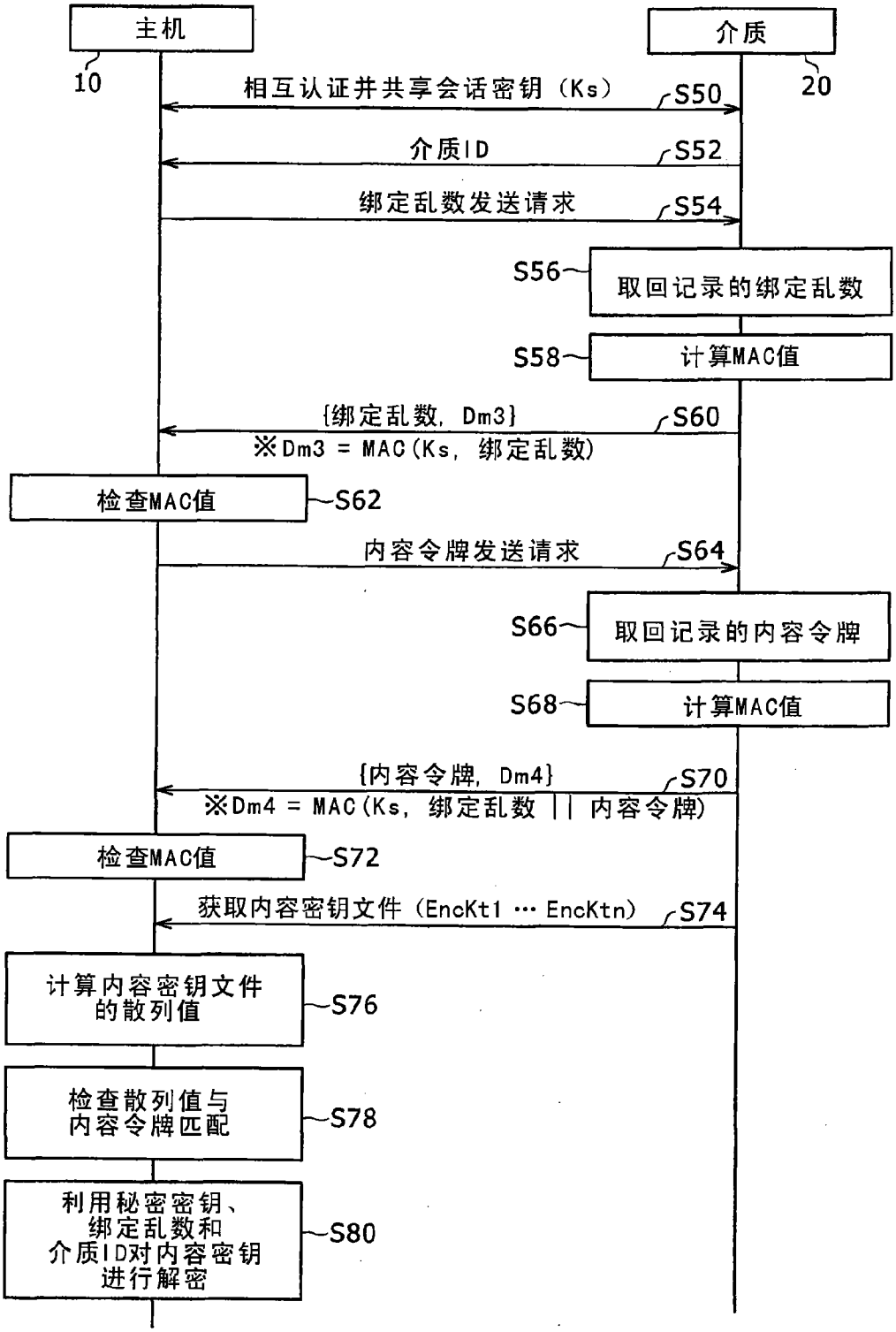

主机
介质
10
20
相互认证并共享会话密钥（Ks）
S50
介质ID
S52
绑定乱数发送请求
S54
S56
取回记录的绑定乱数
S58
计算MAC值
{绑定乱数，Dm3}
S60
※Dm3 = MAC(Ks，绑定乱数)
检查MAC值
S62
内容令牌发送请求
S64
S66
取回记录的内容令牌
S68
计算MAC值
{内容令牌，Dm4}
S70
※Dm4 = MAC(Ks，绑定乱数 || 内容令牌)
检查MAC值
S72
获取内容密钥文件（EncKt1 … EncKtn）
S74
计算内容密钥文件的散列值
S76
检查散列值与内容令牌匹配
S78
利用秘密密钥、绑定乱数和介质ID对内容密钥进行解密
S80

图 7

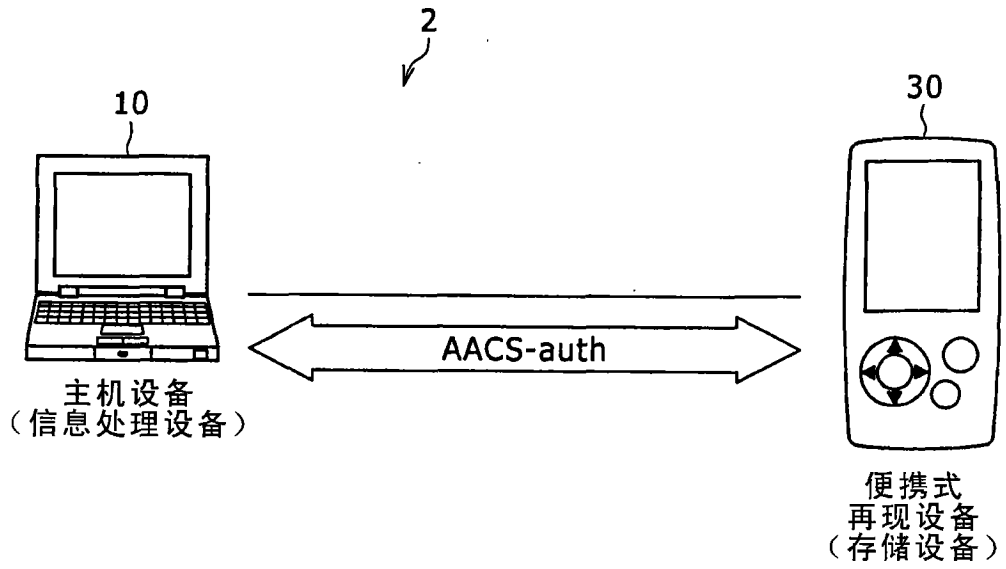



图 8

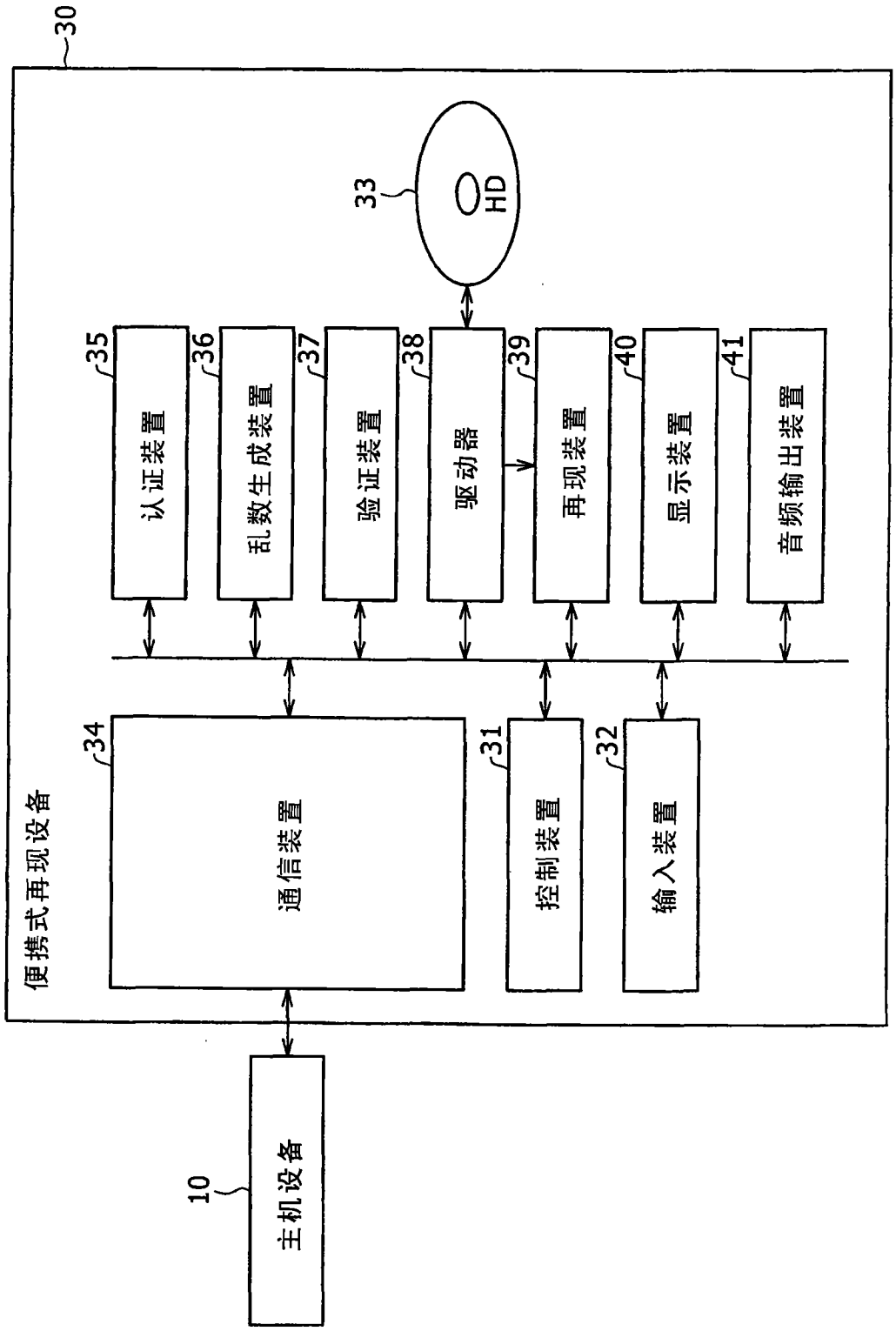

30
便携式再现设备
33
HD
35
认证装置
36
乱数生成装置
37
验证装置
38
驱动器
39
再现装置
40
显示装置
41
音频输出装置
34
通信装置
31
控制装置
32
输入装置
10
主机设备

图9

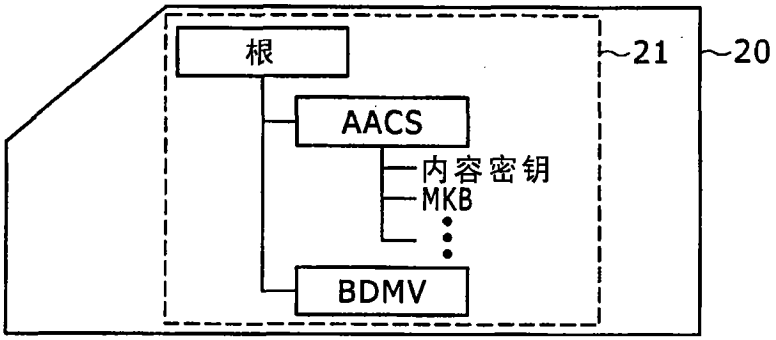



图 10A

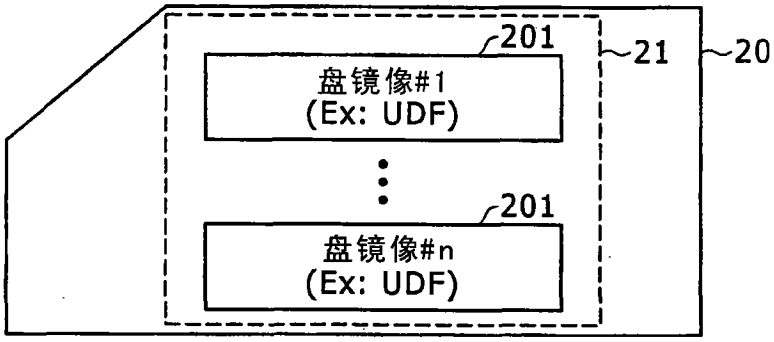



图 10B

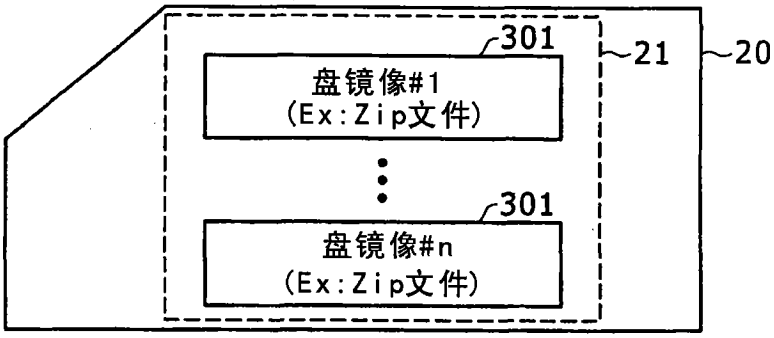



图 10C