(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103220143 A
(43)申请公布日 2013.07.24

(21)申请号 201210448877.8

(22)申请日 2012.11.09

(30)优先权数据
2011-251733 2011.11.17 JP

(71)申请人 索尼公司
地址 日本东京都

(72)发明人 小林义行 久野浩 林隆道

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 康建峰 贾萌

(51)Int.Cl.
H04L 9/32(2006.01)

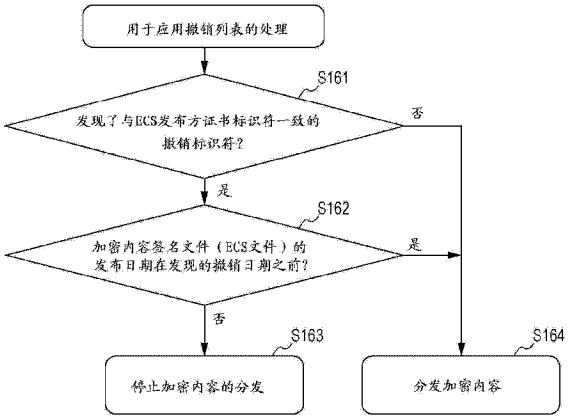
权利要求书5页 说明书42页 附图33页

(54)发明名称

信息处理设备、系统、方法和程序，以及信息存储设备

(57)摘要

本发明提供一种信息处理设备、系统、方法和程序，以及信息存储设备。信息处理设备包括执行用于解码和再现加密内容的处理的数据处理单元。数据处理单元通过应用加密内容签名文件来执行用于确定是否能再现内容的处理。加密内容签名文件存储有加密内容签名文件的发布日期信息和具有加密内容签名发布方的公共密钥的加密内容签名发布方证书。在确定是否能再现内容时，数据处理单元执行下列操作：将加密内容签名发布方证书截止日期与加密内容签名文件的发布日期信息进行比较，当截止日期在发布日期之前时，不执行用于解码和再现加密内容的处理，以及仅当截止日期不在发布日期之前时，执行用于解码和再现加密内容的处理。



CN 103220143 A

1. 一种信息处理设备，包括：

数据处理单元，执行用于解码和再现加密内容的处理，

其中，所述数据处理单元通过应用与要再现的内容相对应设置的加密内容签名文件来执行用于确定内容是否能被再现的处理，

其中，所述加密内容签名文件是这样的文件，其上存储有：

所述加密内容签名文件的发布日期信息，以及

具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

其中，在用于确定所述内容是否能被再现的所述处理中，所述数据处理单元：

将记录在所述加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与所述加密内容签名文件的发布日期信息进行比较，

当所述加密内容签名发布方证书的截止日期在所述加密内容签名文件的发布日期之前时，不执行用于解码和再现所述加密内容的处理，以及

仅当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，执行用于解码和再现所述加密内容的处理。

2. 根据权利要求 1 所述的信息处理设备，其中，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，所述数据处理单元还：

参考撤销列表，所述撤销列表记录有所述加密内容签名发布方证书的失效的信息，以及

在确认所述加密内容签名发布方证书的标识符未被登记在所述撤销列表中的条件下，执行用于解码和再现所述加密内容的处理。

3. 根据权利要求 1 所述的信息处理设备，其中，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，所述数据处理单元还：

参考撤销列表，所述撤销列表记录有所述加密内容签名发布方证书的失效的信息，以及

当所述加密内容签名发布方证书的标识符被登记在所述撤销列表中时，从所述撤销列表获取所述加密内容签名发布方证书的失效日期，并且在确认所述加密内容签名文件的发布日期在所述失效日期之前的条件下，执行用于解码和再现所述加密内容的处理。

4. 根据权利要求 1 所述的信息处理设备，其中，

所述加密内容签名文件是这样的文件，其包括：内容的哈希值；以及用于包括应用于所述内容的解码的密钥信息和所述加密内容签名文件的发布日期的信息的数据的电子签名；以及

在通过对所述电子签名执行签名验证确认所述加密内容签名文件未作假之后，所述数据处理单元执行用于确定所述内容是否能被再现的处理。

5. 根据权利要求 1 所述的信息处理设备，其中，

所述加密内容签名发布方证书中设置有许可发布方的电子签名，

在通过对电子签名执行签名验证确认所述加密内容签名发布方证书未作假之后，所述

数据处理单元执行用于确定所述内容是否能被再现的处理。

6. 一种信息处理设备，包括：

数据处理单元，执行用于向用户装置提供加密内容的处理，

其中，所述数据处理单元通过应用与加密内容对应设置的加密内容签名文件来执行用于确定所述内容是否能被提供的处理，

其中，所述加密内容签名文件是这样的文件，其上存储有：

所述加密内容签名文件的发布日期的信息，以及

具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

其中，在用于确定所述内容是否能被提供的处理中，所述数据处理单元：

将记录在所述加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与所述加密内容签名文件的发布日期的信息进行比较，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，参考记录有所述加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定所述内容是否能被提供的处理，以及

当确认所述加密内容签名发布方证书的截止日期在所述加密内容签名文件的发布日期之前时，参考所述加密内容签名发布方证书的截止日期的信息，执行用于确定所述内容是否能被提供的处理。

7. 根据权利要求 6 所述的信息处理设备，其中，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，所述数据处理单元将所述加密内容签名发布方证书的截止日期与实际时间进行比较，如果所述加密内容签名发布方证书的截止日期在所述实际时间之前，则所述数据处理单元不执行用于向所述用户装置提供所述加密内容的处理。

8. 根据权利要求 6 所述的信息处理设备，其中，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，所述数据处理单元将所述加密内容签名发布方证书的截止日期与实际时间进行比较，当所述加密内容签名发布方证书的截止日期不在所述实际时间之前时，将所述加密内容签名文件的发布日期与实际时间进行比较，当所述加密内容签名文件的发布日期在所述实际时间之前时，不执行用于向所述用户装置提供所述加密内容的处理。

9. 根据权利要求 8 所述的信息处理设备，其中，

当确认所述加密内容签名文件的发布日期不在所述实际时间之前时，所述数据处理单元进一步参考其中记录有所述加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理。

10. 根据权利要求 6 所述的信息处理设备，其中，

所述数据处理单元参考其中记录有所述加密内容签名发布方证书的失效的信息的撤销列表，并且在确认所述加密内容签名发布方证书的标识符未被登记在所述撤销列表中的条件下，执行用于向所述用户装置提供所述加密内容的处理。

11. 根据权利要求 6 所述的信息处理设备，其中，

所述数据处理单元参考其中记录有所述加密内容签名发布方证书的失效的信息的撤

销列表来执行用于确定所述内容是否能被提供的处理，当所述加密内容签名发布方证书的标识符被登记在所述撤销列表中时，从所述撤销列表获取所述加密内容签名发布方证书的失效日期，并且在确认所述加密内容签名文件的发布日期在所述失效日期之前的条件下，执行用于向所述用户装置提供所述加密内容的处理。

12. 一种信息处理系统，包括：

用户装置，其执行用于再现内容的处理；

内容提供方，其执行用于将内容提供给所述用户装置的处理；以及

加密内容签名发布方，其执行用于将加密内容签名文件提供给所述内容提供方的处理，其中，

所述内容提供方将内容哈希列表集和内容加密密钥或所述加密密钥的哈希值发送到所述加密内容签名发布方，所述内容哈希列表集包括以所述内容的配置数据为基础的哈希值，

所述加密内容签名发布方：生成用于作为签名目标的数据的签名数据，作为签名目标的数据是包括所述内容哈希列表集、所述内容加密密钥的哈希值和生成加密内容签名文件的日期的信息的数据；生成包括所生成的签名数据和所述内容哈希列表集的加密内容签名文件；以及将所述加密内容签名文件发送给所述内容提供方，

所述内容提供方通过应用生成所述加密内容签名文件的日期的信息来执行用于确定内容是否能被提供的处理，以及

所述用户装置通过应用生成所述加密内容签名文件的日期的信息来执行用于确定所述内容是否能被再现的处理。

13. 一种信息存储设备，包括：

存储单元，其存储加密内容和将用于所述加密内容的解码的加密密钥，其中，

所述存储单元包括保护区和通用区，所述保护区上存储有作为所述加密密钥的转换数据的转换加密密钥，所述保护区设置有访问限制，并且所述通用区上存储有所述加密内容，

所述通用区上存储有与所述加密内容对应设置的加密内容签名文件，

所述加密内容签名文件是这样的文件，其上存储有：所述加密内容签名文件的发布日期的信息，以及具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

使执行用于从所述存储单元读取并且再现所述加密内容的处理的再现设备通过应用所述加密内容签名文件的发布日期的信息来确定所述内容是否能被再现。

14. 根据权利要求 13 所述的信息存储设备，其中

所述加密内容签名文件包括用于所述发布日期的信息的电子签名，以及

使执行用于从所述存储单元读取并且再现所述加密内容的处理的所述再现设备对所述加密内容签名文件的所述电子签名执行验证处理，并且在成功进行验证的条件下，通过应用所述发布日期的信息来确定所述内容是否能被再现。

15. 一种在信息处理设备中实现的信息处理方法，其中

所述信息处理设备包括执行用于解码和再现加密内容的处理的数据处理单元，

所述数据处理单元通过应用与要再现的内容对应设置的加密内容签名文件来执行用于确定所述内容是否能被再现的处理，

所述加密内容签名文件是这样的文件，其上存储有：所述加密内容签名文件的发布日期的信息，以及具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

在用于确定所述内容是否能被再现的所述处理中，所述数据处理单元：

将记录在所述加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与所述加密内容签名文件的发布日期的信息进行比较，

当所述加密内容签名发布方证书的截止日期在所述加密内容签名文件的发布日期之前时，不执行用于解码和再现所述加密内容的处理，以及

仅当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，执行用于解码和再现所述加密内容的处理。

16. 一种在信息处理设备中实现的信息处理方法，其中

所述信息处理设备包括执行用于将加密内容提供给用户装置的处理的数据处理单元，

所述数据处理单元通过应用设置为与所述加密内容相对应的加密内容签名文件来执行用于确定所述内容是否能被提供的处理，

所述加密内容签名文件是这样的文件，其上存储有：所述加密内容签名文件的发布日期的信息，以及具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

其中，在用于确定所述内容是否能被提供的处理中，所述数据处理单元：

将记录在所述加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与所述加密内容签名文件的发布日期的信息进行比较，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，参考其中记录有所述加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定所述内容是否能被提供的处理，以及

当确认所述加密内容签名发布方证书的截止日期在所述加密内容签名文件的发布日期之前时，参考所述加密内容签名发布方证书的截止日期的信息，执行用于确定所述内容是否能被提供的处理。

17. 一种使信息处理设备执行信息处理的程序，其中，

所述信息处理设备包括执行用于解码和再现加密内容的处理的数据处理单元，

所述程序使所述数据处理单元通过应用与要再现的内容对应设置的加密内容签名文件来执行用于确定所述内容是否能被再现的处理，

所述加密内容签名文件是这样的文件，其上存储有：所述加密内容签名文件的发布日期的信息，以及具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

在用于确定所述内容是否能被再现的处理中，所述程序使所述数据处理单元：

将记录在所述加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与所述加密内容签名文件的发布日期的信息进行比较，

当所述加密内容签名发布方证书的截止日期在所述加密内容签名文件的发布日期之前时，不执行用于解码和再现所述加密内容的处理，以及

仅当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发

布日期之前时，执行用于解码和再现所述加密内容的处理。

18. 一种使信息处理设备执行信息处理的程序，其中，

所述信息处理设备包括执行用于将加密内容提供给用户装置的处理的数据处理单元，

所述程序使所述数据处理单元通过应用设置为与所述加密内容相对应的加密内容签名文件来执行用于确定所述内容是否能被提供的处理，

所述加密内容签名文件是这样的文件，其上存储有：所述加密内容签名文件的发布日期的信息，以及具有作为生成所述加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

其中，在用于确定所述内容是否能被提供的处理中，所述程序使所述数据处理单元：

将记录在所述加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与所述加密内容签名文件的发布日期的信息进行比较，

当确认所述加密内容签名发布方证书的截止日期不在所述加密内容签名文件的发布日期之前时，参考其中记录有所述加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定所述内容是否能被提供的处理，以及

当确认所述加密内容签名发布方证书的截止日期在所述加密内容签名文件的发布日期之前时，参考所述加密内容签名发布方证书的截止日期的信息，执行用于确定所述内容是否能被提供的处理。

信息处理设备、系统、方法和程序，以及信息存储设备

技术领域

[0001] 本公开涉及一种信息处理设备、信息存储设备、信息处理系统以及信息处理方法和程序。特别地，本公开涉及一种防止内容不当使用的信息处理设备、信息存储设备、信息处理系统以及信息处理方法和程序。

背景技术

[0002] 例如，诸如电影、音乐等内容通过诸如 DVD（数字通用盘）、蓝光盘（注册商标）和快擦写存储器的各种媒质、诸如互联网的网络或广播波提供给用户。用户可利用诸如PC、移动终端的各种信息处理设备、诸如 BD 播放器的记录和再现设备以及电视机再现内容。

[0003] 然而，被提供给用户的诸如音乐数据和图像数据的大多数内容的版权和发行权由内容的制作者或销售者所有。因此，在很多情况下内容提供方在提供给用户内容时执行预定的内容使用限制。

[0004] 根据数字记录设备和记录介质，例如，能够在不使图像和声音劣化的情况下进行重复记录和再现，并且存在这样的问题：诸如所谓的盗版盘的发行的不当复制内容的使用或经由互联网不当复制内容的传输已经很普遍。

[0005] 为了防止这种不当数据复制，已经实施了用于防止在数字记录设备和记录介质中的非法复制的各种技术。

[0006] 例如，内容加密处理是一个实例。用于解码加密数据的密钥仅被给予被许可具有内容使用权的再现设备。设计成遵循预定操作规则（例如再现设备不执行不当复制）的再现设备被许可。另一方面，不被许可的再现设备不具有用于解码加密数据的密钥，因此，该再现设备不解码加密数据。

[0007] 然而，即使执行这种内容加密，在当前情形下内容仍被不当使用。

[0008] 将说明内容不当使用的一个特定实例。

[0009] 设想如下配置：内容服务器将加密内容传输给诸如记录和再现设备、PC 或移动终端的用户装置。

[0010] 当内容服务器向用户装置传输加密内容时，内容服务器例如经由网络向用户装置传输如下数据：（a）加密内容，和（b）应用于加密内容的加密和解码的加密密钥。

[0011] 例如，当诸如相同电影的相同内容被提供给多个用户装置时，内容服务器执行如下两种处理。（A）内容服务器通过应用不同的独立加密密钥而生成不同的加密内容并且将其提供给用户装置。（B）内容服务器生成已经利用同样的加密密钥加密的同样的加密内容并且将其提供给多个用户装置。

[0012] 考虑到用于防止内容不当使用的安全性，上述处理（A）是有效的。

[0013] 然而，为了执行上述处理（A），需要执行为多个用户设置独立加密密钥并且生成独立加密内容的处理，存在如下问题：随着内容传输到的用户数目的增大，服务器的处理负担增大，处理负担诸如为加密密钥的生成和管理、加密内容生成处理等。

[0014] 因此，在很多情形下执行上述处理（B），即对于同样的内容生成利用同样的加密密

钥加密的同样的加密内容并且将加密内容提供给多个用户装置。

[0015] 例如，为具有某一标题的内容设置一个加密密钥(=标题密钥)，应用该一个标题密钥以生成相同的加密内容，并且将(a)加密内容和(b)标题密钥的数据集传输给多个用户。

[0016] 通过执行这种处理，减小内容服务器的处理负担。

[0017] 下文中，将以内容标题为单位设置的加密密钥描述为“标题密钥”。

[0018] 另外，标题密钥被应用到具有标题的加密内容的加密和解码处理。

[0019] 然而，如果将同样的数据集(即同样的(a)加密内容和(b)标题密钥的数据的组合)传输给多个用户，则作为用户一部分中的“未授权用户”可以执行下述处理：

[0020] (1)“未授权用户”读取从服务器接收到的标题密钥，并且将读取的标题密钥发布至不定数目的用户；或者

[0021] (2)“未授权用户”使用与某一加密内容 A 对应的标题密钥 A 加密完全不同的内容 B，并且将(X)标题密钥 A 和(Y)利用标题密钥 A 加密的加密内容 B 的数据组合传输给不定数目的用户。

[0022] 存在如下执行不当使用的可能性。

[0023] 例如，如果执行上述处理(1)，则获取不当发布的标题密钥的多个用户使用已经利用标题密钥不当加密的内容。

[0024] 另外，如果执行上述处理(2)，则从“未授权用户”获得由“未授权用户”生成的不当数据集(即(X)标题密钥 A 和(Y)利用标题密钥 A 加密的加密内容 B)，并且多个用户使用不当加密的内容 B。

[0025] 结果，合法购买原始合法数据集(即加密内容B和与加密内容B对应的标题密钥B)的用户数目减少，显著损害了版权所有人的权益和发行权所有人的权益。

[0026] 将给出不当处理的实例的另一具体说明。

[0027] 设想内容服务器拥有下述(1)-(3)的加密内容 C 和标题密钥(Kt)的数据集。(1)(Kt11,C11)；(2)(Kt12,C12)；(3)(Kt13,C13)。其中，Cnn 表示内容文件，Ktnn 表示在加密内容中使用的标题密钥。(Kt11,C11)是标题密钥(Kt11)和利用标题密钥(Kt11)加密的内容(C11)的数据集。

[0028] 例如，假定“未授权用户 Ux”购买了全部上述三个数据集，即(1)(Kt11,C11)；(2)(Kt12,C12)；(3)(Kt13,C13)。

[0029] 假定购买处理本身是通过诸如 PC 的“未授权用户 Ux”的用户装置和内容服务器之间的预定的适当购买程序执行的。

[0030] “未授权用户 Ux”在诸如作为用户装置的 PC 的介质(诸如硬盘)中记录上述数据集(1)-(3)。

[0031] “未授权用户 Ux”从诸如作为用户装置 PC 的 PC 硬盘的介质中读取上述数据集(1)-(3)，并且利用其自己的标题密钥一次将所有的加密内容全部解码，以获取下列数据：

[0032] 标题密钥：Kt11、Kt12、Kt13；

[0033] 解码内容：C11、C12、C13。

[0034] 尽管当在适当再现设备中使用合法内容再现程序时标题密钥通常不被读取到外部，但是存在如下可能性：标题密钥自身可被通过在诸如 PC 的设备上安装不当程序的方法来读取，在当前情形下，难以完全防止标题密钥被读取。

[0035] 此外，“未授权用户 Ux”生成通过耦合（couple）解码内容 C11-C13 来获得的数据 C11||C12||C13，并且利用标题密钥 kt11 加密耦合的数据。

[0036] 也就是，“未授权用户 Ux”生成下述数据集（Kt11, C11||C12||C13），并且经由网络不当地发布该数据集，例如，以便宜的价格销售该数据集，或者将数据集免费提供给很多用户。

[0037] 如果执行这种处理，则很多一般用户可以从“未授权用户 Ux”获取上述不当生成的数据集，即不当数据集（Kt11, C11||C12||C13）。

[0038] 数据集是由（a）利用标题密钥 Kt11 加密的加密内容和（b）标题密钥 Kt11 配置而成，并且数据配置与从合法内容提供方提供给用户的数据集中的内容的数据配置相同。

[0039] 因此，包括适当内容再现程序的适当许可的再现设备可以使用标题密钥 Kt11 毫无任何问题的解码和再现加密内容（C11||C12||C13）。

[0040] 结果，内容未被合法购买，不当使用广泛传播。由于合法购买内容 C11-C13 的用户数目下降，损害适当权利拥有者的权益。

[0041] 将给出另一具体说明。例如，在诸如戏曲的包括从第一幕到第十二幕的十二个标题的系列内容的情况中，假定以幕为单位设置内容购买单位如下：

[0042] 第一幕 =（Kt01, C01）；

[0043] 第二幕 =（Kt02, C02）；

[0044] 第三幕 =（Kt03, C04）；

[0045] …；

[0046] 第十二幕 =（Kt12, C12）。

[0047] 在这种情况下，“未授权用户”购买系列中的从第一幕到第十二幕的全部十二个标题，耦合第一幕至第十二幕的内容 C01-C12，生成利用与第一幕对应的标题密钥 Kt01 再次加密的数据集，即（Kt01, C01||C02||C03…||C12），并将数据集发布在网络上。或者，未授权用户执行不当销售数据集的处理。

[0048] 在这种情况下，多个用户装置能获取、再现和使用由“未授权用户”生成的不当数据集，即（Kt01, C01||C02||C03…||C12）。

[0049] 例如，假定十二幕中的每一幕的合法价格为 2,000 日元。

[0050] 在这种情况下，全部十二幕的价格为 12×2,000 日元 =24,000 日元。

[0051] “未授权用户”例如以 6,000 日元的价格销售不当数据集，即（Kt01, C01||C02||C03…||C12）。在这种情况下，很多用户购买较便宜的内容，结果，扰乱合法内容销售，损害原始拥有版权和销售权的所有者的利益和权利。

[0052] 除上述实例之外，可以使用与某一内容 C11 的一段相对应设置的标题密钥 Kt11 编码其它各种不具有任何关系的内容 Cxx，如（Kt11, Cxx），内容 Cxx 可以是各种内容，存在如下问题：所有内容可无限制地利用一个标题密钥解码和再现。

[0053] 也就是，即使生产出的再现设备被禁止再现纯文本内容，也能够使用以与合法购买内容一样的方式设置的不当数据集来解码和再现纯文本内容。

[0054] 此外，“未授权用户”可启动替换标题密钥并且再次加密内容的服务，并且能够像是授权服务器那样行事。

[0055] 如上所述，难以仅利用内容加密处理的对策来防止内容的不当使用。

[0056] 作为除加密处理之外消除内容不当使用的方法，存在如下方法：使得再现设备执行内容的伪造（falsity）验证。通过应用该方法，例如，当不当内容的发行处理中对内容进行任何修改（伪造）时，能阻止使用伪造的内容。

[0057] 具体地，再现内容的用户装置被设计成具有受控的配置，其中，使用户装置执行用于验证是否存在内容伪造的处理，以仅在确认内容无伪造时才再现内容，且当确定内容伪造时则不再现内容。

[0058] 例如，日本未审查专利申请公报 2002-358011 号公开了一种受控配置，其中，从将再现的内容文件计算哈希值（hash value），将该哈希值与预先准备的用于交叉校验的哈希值（即基于适当内容数据预先计算出的用于交叉校验的哈希值）进行比较，当新计算出的哈希值与用于交叉校验的哈希值一致时确定内容没有被伪造，并且处理进行到内容再现处理。

[0059] 然而，如果在执行如上所述的用于基于内容计算哈希值的处理时作为用于计算哈希值的原始数据的内容数据的容量大，则计算所需的处理负担明显加大，并且处理时间明显变长。近来，视频图像数据品质高，单位内容的数据量在很多情况下是从几个 GB 到几十 GB 的范围。存在如下问题：用户装置需要具有显著的高的数据处理能力；如果使再现内容的用户装置执行这种用于基于大容量数据计算内容的哈希值的处理，则由于内容验证时间长，不能有效地执行内容再现处理。

[0060] 另外，日本专利 4576936 号公开了一种配置，其中，被设置为信息记录介质上的存储内容的分类数据的每个哈希单元的哈希值被记录在内容哈希表中，内容哈希表与内容一起存储在信息记录介质上。

[0061] 利用这种公开的配置，再现内容的信息处理设备基于一个或更多随机选择的哈希单元（hash unit）来执行用于交叉校验哈希值的处理。利用这种配置，能利用较少量的数据基于哈希单元计算哈希值，以与内容数据量无关地执行交叉校验处理，从而通过再现内容的用户装置有效地验证内容。

[0062] 然而，日本专利 4576936 号中公开的配置假定所处理的内容存储在信息记录介质上。尽管公开的配置可适用于可在制造信息记录介质时将哈希值与内容记录在一起的情况，但是，例如存在难以将该配置应用于例如从服务器下载的内容的问题。

[0063] 日本未审查专利申请公报 2002-358011 号和日本专利 4576936 号都重视内容伪造验证，但是存在如下问题：不当复制的未伪造的内容的发布一点也不受控制。

[0064] 如上所述，在当前形势下，相关技术中的内容加密和伪造验证处理在防止不当复制内容的发布方面以及内容加密密钥的泄露方面未能展示足够好的效果。

发明内容

[0065] 期望提供一种信息处理设备、信息存储设备、信息处理系统以及信息处理方法和程序，其能有效防止内容不当使用。

[0066] 根据本公开的第一实施例，提供一种信息处理设备包括：数据处理单元，执行用于解码和再现加密内容的处理，其中，数据处理单元通过应用与要再现的内容相对应设置的加密内容签名文件来执行用于确定内容是否能被再现的处理，其中，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期信息，以及具有作为生成加密内容

签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，其中，在用于确定内容是否能被再现的处理中，数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期信息进行比较，当加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，不执行用于解码和再现加 密内容的处理，以及仅当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，执行用于解码和再现加密内容的处理。

[0067] 此外，在根据该实施例的信息处理设备中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元还：参考撤销列表，撤销列表记录有加密内容签名发布方证书的失效的信息，以及在确认加密内容签名发布方证书的标识符未被登记在撤销列表中的条件下，执行用于解码和再现加密内容的处理。

[0068] 此外，在根据该实施例的信息处理设备中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元还：参考撤销列表，撤销列表记录有加密内容签名发布方证书的失效的信息，以及当加密内容签名发布方证书的标识符被登记在撤销列表中时，从撤销列表获取加密内容签名发布方证书的失效日期，并且在确认加密内容签名文件的发布日期在失效日期之前的条件下，执行用于解码和再现加密内容的处理。

[0069] 此外，在根据该实施例的信息处理设备中，加密内容签名文件是这样的文件，其包括：内容的哈希值；以及用于包括应用于内容的解码的密钥信息和加密内容签名文件的发布日期的信息的数据的电子签名；以及在通过对电子签名执行签名验证确认加密内容签名文件未作假之后，数据处理单元执行用于确定内容是否能被再现的处理。

[0070] 此外，在根据该实施例的信息处理设备中，加密内容签名发布方证书中设置有许可发布方的电子签名，在通过对电子签名执行签名验证确认加密内容签名发布方证书未作假之后，数据处理单元执行用于确定内容是否能被再现的处理。

[0071] 根据本发明的第二实施例，提供一种信息处理设备，包括：数据处理单元，执行用于向用户装置提供加密内容的处理，其中，数据处理单元通过应用与加密内容对应设置的加密内容签名文件来执行用于确定内容是否能被提供的处理，其中，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，其中，在用于确定内容是否能被提供的处理中，数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期的信息进行比较，当确认加密内容签名发布方 证书的截止日期不在加密内容签名文件的发布日期之前时，参考记录有加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理，以及当确认加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，参考加密内容签名发布方证书的截止日期的信息，执行用于确定内容是否能被提供的处理。

[0072] 此外，在根据该实施例的信息处理设备中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元将加密内容签名发布方证书的截止日期与实际时间进行比较，如果加密内容签名发布方证书的截止日期在实际时间之前，则数据处理单元不执行用于向用户装置提供加密内容的处理。

[0073] 此外，在根据该实施例的信息处理设备中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元将加密内容签名发布方证书的截止日期与实际时间进行比较，当加密内容签名发布方证书的截止日期不在实际时间之前时，将加密内容签名文件的发布日期与实际时间进行比较，当加密内容签名文件的发布日期在实际时间之前时，不执行用于向用户装置提供加密内容的处理。

[0074] 此外，在根据该实施例的信息处理设备中，当确认加密内容签名文件的发布日期不在实际时间之前时，数据处理单元进一步参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理。

[0075] 此外，在根据该实施例的信息处理设备中，数据处理单元参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表，并且在确认加密内容签名发布方证书的标识符未被登记在撤销列表中的条件下，执行用于向用户装置提供加密内容的处理。

[0076] 此外，在根据该实施例的信息处理设备中，数据处理单元参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表来执行用于确定内容是否能被提供的处理，当加密内容签名发布方证书的标识符被登记在撤销列表中时，从撤销列表获取加密内容签名发布方证书的失效日期，并且在确认加密内容签名文件的发布日期在失效日期之前的条件下，执行用于向用户装置提供加密内容的处理。

[0077] 根据本发明的第三实施例，提供一种信息处理系统，包括：用户装置，其执行用于再现内容的处理；内容提供方，其执行用于将内容提供给用户 装置的处理；以及加密内容签名发布方，其执行用于将加密内容签名文件提供给内容提供方的处理，其中，内容提供方将内容哈希列表集和内容加密密钥或加密密钥的哈希值发送到加密内容签名发布方，内容哈希列表集包括以内容的配置数据为基础的哈希值，加密内容签名发布方：生成用于作为签名目标的数据的签名数据，作为签名目标的数据是包括内容哈希列表集、内容加密密钥的哈希值和生成加密内容签名文件的日期的信息的数据；生成包括所生成的签名数据和内容哈希列表集的加密内容签名文件；以及将加密内容签名文件发送给内容提供方，内容提供方通过应用生成加密内容签名文件的日期的信息来执行用于确定内容是否能被提供的处理，以及用户装置通过应用生成加密内容签名文件的日期的信息来执行用于确定内容是否能被再现的处理。

[0078] 根据本发明的第四实施例，提供一种信息存储设备，包括：存储单元，其存储加密内容和将用于加密内容的解码的加密密钥，其中，存储单元包括保护区和通用区，保护区上存储有作为加密密钥的转换数据的转换加密密钥，保护区设置有访问限制，并且通用区上存储有加密内容，通用区上存储有与加密内容对应设置的加密内容签名文件，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，使执行用于从存储单元读取并且再现加密内容的处理的再现设备通过应用加密内容签名文件的发布日期的信息来确定内容是否能被再现。

[0079] 此外，在根据该实施例的信息处理设备中，加密内容签名文件包括用于发布日期的信息的电子签名，以及使执行用于从存储单元读取并且再现加密内容的处理的再现设备对加密内容签名文件的电子签名执行验证处理，并且在成功进行验证的条件下，通过应用发布日期的信息来确定内容是否能被再现。

[0080] 根据本发明的第五实施例，提供一种在信息处理设备中实现的信息处理方法，其中信息处理设备包括执行用于解码和再现加密内容的处理的数据处理单元，数据处理单元通过应用与要再现的内容对应设置的加密内容签名文件来执行用于确定内容是否能被再现的处理，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，在用于确定内容是否能被再现的处理中，数 据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期的信息进行比较，当加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，不执行用于解码和再现加密内容的处理，以及仅当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，执行用于解码和再现加密内容的处理。

[0081] 根据本发明的第六实施例，提供一种在信息处理设备中实现的信息处理方法，其中信息处理设备包括执行用于将加密内容提供给用户装置的处理的数据处理单元，数据处理单元通过应用设置为与加密内容相对应的加密内容签名文件来执行用于确定内容是否能被提供的处理，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，其中，在用于确定内容是否能被提供的处理中，数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期的信息进行比较，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理，以及当确认加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，参考加密内容签名发布方证书的截止日期的信息，执行用于确定内容是否能被提供的处理。

[0082] 根据本发明的第七实施例，提供一种使信息处理设备执行信息处理的程序，其中，信息处理设备包括执行用于解码和再现加密内容的处理的数据处理单元，程序使数据处理单元通过应用与要再现的内容对应设置的加密内容签名文件来执行用于确定内容是否能被再现的处理，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，在用于确定内容是否能被再现的处理中，程序使数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期的信息进行比较，当加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，不执行用于解码和再现加密内容的处理，以及仅当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，执行用于解码和再现加密内容的处理。

[0083] 根据本发明的第八实施例，提供一种使信息处理设备执行信息处理的程序，其中，信息处理设备包括执行用于将加密内容提供给用户装置的处理的数据处理单元，程序使数据处理单元通过应用设置为与加密内容相对应的加密内容签名文件来执行用于确定内容是否能被提供的处理，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公

共密钥的加密内容签名发布方证书，其中，在用于确定内容是否能被提供的处理中，程序使数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期的信息进行比较，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理，以及当确认加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，参考加密内容签名发布方证书的截止日期的信息，执行用于确定内容是否能被提供的处理。

附图说明

[0084] 图 1A 至图 1C 是例示内容提供处理和使用处理的概略的图；

[0085] 图 2 是例示记录在存储卡中的内容的使用状态的图；

[0086] 图 3 是例示存储卡中的存储区的具体配置实例的图；

[0087] 图 4 是例示主机证书的图；

[0088] 图 5 是例示服务器证书的图；

[0089] 图 6 是例示存储在存储卡上的数据的具体配置实例和访问控制处理实例的图；

[0090] 图 7 是例示本公开的防止内容不当使用的信息处理系统的整体配置的图；

[0091] 图 8 是例示适于防止内容不当使用的设备之间的数据流的图；

[0092] 图 9A 和图 9B 是例示加密内容签名文件（ECS 文件）的配置实例的图；

[0093] 图 10 是例示加密内容签名文件（ECS 文件）的配置实例的图；

[0094] 图 11 是例示包含在加密内容签名文件（ECS 文件）中的 ECS 发布方证书的配置实例的图；

[0095] 图 12 是 ECS 发布方证书撤销列表的配置实例的图；

[0096] 图 13 是例示用于生成加密内容签名文件（ECS 文件）和数据配置的处理的概略的图。

[0097] 图 14 是例示加密内容签名文件（ECS 文件）的生成、内容的提供和使用处理序列的序列图；

[0098] 图 15 是例示加密内容签名文件（ECS 文件）的生成、内容的提供和使用处理序列的序列图；

[0099] 图 16 是示出例示用于通过应用记录在加密内容签名文件（ECS 文件）中的日期数据来确定是否能提供内容的处理的序列的流程的图。

[0100] 图 17 是示出例示用于通过应用记录在加密内容签名文件（ECS 文件）中的日期数据来确定是否能提供内容的处理的序列的流程的图。

[0101] 图 18 是示出例示用于通过应用记录在加密内容签名文件（ECS 文件）中的日期数据来确定是否能再现内容的处理的序列的流程的图。

[0102] 图 19 是例示用于通过服务器在存储卡中记录数据的处理实例的图；

[0103] 图 20 是例示用于通过主机读取存储卡中的数据的处理实例的图；

[0104] 图 21 是例示记录在存储卡中的数据的配置实例的图；

[0105] 图 22 是例示记录在存储卡中的数据的配置实例的图；

[0106] 图 23 是例示关于记录在存储卡中的通用区中的使用规则的记录数据的配置实例

的图；

[0107] 图 24 是例示使用通过替换处理使用不当内容的实例的图；

[0108] 图 25 是示出例示用于通过替换处理来记录不当内容的处理的实例的流程的图；

[0109] 图 26 是示出例示不再现通过替换处理记录的不当内容的流程图的图；

[0110] 图 27 是例示通过替换处理使用不当内容的实例的图；

[0111] 图 28 是示出例示用于通过替换处理来记录不当内容的处理实例的流程图的图；

图 29 是示出例示用户装置再现内容 C1 时的处理的流程图的图；

[0112] 图 30 是例示记录在加密内容签名文件（ECS 文件）中的块标识符和记录在使用规则文件中的块标识符的图；

[0113] 图 31 是示出例示通过应用记录在加密内容签名文件（ECS 文件）中的块标识符和记录在使用规则文件中的块标识符来确定内容是否能被提供的序列的流程图的图；

[0114] 图 32 是示出例示用于从 ECS 发布方证书读取块标识符的处理序列的流程图的图；

[0115] 图 33 是示出例示通过应用记录在加密内容签名文件（ECS 文件）中的块标识符和记录在使用规则文件中的块标识符来确定内容是否能被再现的序列的流程图的图；

[0116] 图 34 是例示信息处理设备的硬件配置实例的图；以及

[0117] 图 35 是例示作为存储卡的信息处理设备的硬件配置的图。

具体实施方式

[0118] 下文中，将参照附图对根据本公开的信息处理设备、信息存储设备、信息处理系统以及信息处理方法和程序进行详细说明。另外，将对下列诸项进行说明：1、用于提供内容的处理和用于使用内容的处理的概略；2、关于存储卡的配置实例和使用实例；3、关于包括保护区访问允许信息的证书；4、关于用于通过应用每个设备的证书来访问存储卡的处理的实例；5、关于利用加密内容签名（ECS）发布方的内容提供系统；6、关于 ECS 文件的配置实例；7、关于 ECS 发布方证书撤销列表的配置；8、关于用于生成加密内容签名文件（ECS 文件）的处理；9、关于应用 ECS 文件和 ECS 发布方证书的日期信息的处理；10、关于关联加密密钥和 ECS 发布方签名的配置；11、关于用于应用记录在加密内容签名（ECS）文件中的块标识符的处理；12、关于各个设备的硬件配置实例；13、根据本公开的配置的结论。

[0119] [1. 用于提供内容的处理和用于使用内容的处理的概略]

[0120] 下文中，将参照附图说明本公开的信息处理设备及信息处理方法和程序。

[0121] 首先，将参照图 1A 至图 1C 说明用于提供内容的处理和用于使用内容的处理的概略。

[0122] 图 1A 示出内容提供方的实例，图 1B 示出内容记录和再现设备（主机）的实例，图 1C 示出内容记录介质的实例。

[0123] 图 1C 中的内容记录介质是用户记录内容的介质，其在用于再现内容的处理中使用。这里，存储卡 31 示例为诸如快擦写存储器的信息存储设备。

[0124] 另外，尽管在下列的实施例中以内容提供方所提供的内容是加密内容的实施例进行说明，但是本发明公开的配置不限于提供的内容是加密内容的情形，也可适用于未加密的纯文本内容的情况。

[0125] 用户在存储卡 31 中记录和使用诸如音乐和电影的各种内容。这种内容例如包括作为使用控制目标的内容，诸如作为版权管理目标的内容。

[0126] 作为使用控制目标的内容是指使用时段受限的内容、复制数据未受管理的复制或发布被禁止的内容等。另外，当在存储卡 31 中记录使用受控制的内容时，与内容对应的使用规则被一起记录。

[0127] 在使用规则中，记录有与诸如允许内容使用时段、允许复制次数等内容使用有关的信息。

[0128] 内容提供方根据内容来提供内容使用规则。

[0129] 在图 1A 中，内容提供方是音乐、电影等的内容提供方。在图 1A 中，广播站 11 和内容服务器 12 被示出为内容提供方。

[0130] 广播站 11 例如是电视台，其在地波上或经由卫星的卫星波上向用户装置（图 1B 中的内容记录和再现设备（主机））提供各种广播内容。

[0131] 内容服务器 12 是经由诸如互联网的网络提供诸如音乐或电影的内容的服务器。

[0132] 用户可将图 1C 中的作为内容记录介质的存储卡 31 安装在图 1B 中的内容记录和再现设备（主机）上，经由位于图 1B 中的内容记录和再现设备（主机）自身上的接收单元或连接到内容记录和再现设备（主机）的接收设备接收由广播站 11 或内容服务器 12 提供的内容，并且将内容记录在存储卡 31 中。

[0133] 在图 1B 中的内容记录和再现设备（主机）上安装图 1C 中的作为内容记录介质的存储卡 31，并且将从图 1A 中的作为内容提供方的广播站 11 或内容服务器 12 接收的内容记录在存储卡 31 中。

[0134] 图 1B 中的内容记录和再现设备（主机）的实例包括设置有硬盘和诸 如 DVD 播放器的 DVD 或 BD 盘的记录和再现专用装置（CE 装置 ：消费者电子装置）21。此外，实例包括 PC 22 和诸如智能手机、移动手机、移动播放器、或平板终端的移动终端 23。所有这些实例设计成其上可安装图 1C 中的作为内容记录介质的存储卡 31。

[0135] 用户利用记录和再现专用装置 21、PC 22、移动终端 23 等从广播站 11 或内容服务器 12 接收诸如音乐或电影的内容，并且将内容记录在存储卡 31 中。

[0136] 将参照图 2 说明记录在存储卡 31 中的内容的使用状态。

[0137] 用作信息存储设备的存储卡 31 是可拆卸地安装到诸如 PC 的内容再现装置的记录介质，并且可以从记录有内容的设备自由拆下，以安装到另一用户装置。

[0138] 也就是，如图 2 所示，存储卡 31 执行（1）记录处理和（2）再现处理。

[0139] 另外，也存在仅执行记录或再现之一的设备。

[0140] 另外，同一设备既执行记录处理又执行再现处理是不必要的，用户可以自由地选择和使用记录设备和再现设备。

[0141] 另外，记录在存储卡 31 中的受限内容在很多情况下被记录为加密内容，诸如记录和再现专用装置 21、PC 22 或移动终端 23 的内容再现设备基于预定的序列执行解码处理，然后再现内容。

[0142] 另外，当处于在与内容对应设置的使用规则中记录的使用允许状态下，内容再现设备执行再现处理。

[0143] 图 1B 中的内容记录和再现设备（主机）在其上存储用于基于使用规则执行内容使

用和内容解码处理的程序(主机应用程序),基于程序(主机应用程序)执行内容再现。

[0144] [2. 关于存储卡的配置实例和使用实例]

[0145] 接下来,将对用作内容记录介质的诸如快擦写存储器的存储卡的配置实例和使用实例进行说明。

[0146] 图 3 示出存储卡 31 中的存储区的具体配置实例。

[0147] 如图 3 所示,存储卡 31 中的存储区由两个区域配置而成,即(a)保护区 51 和(b)通用区 52。

[0148] (b)通用区 52 是可被用户所使用的记录和再现设备自由访问并记录内容、与内容对应的使用规则、其它通用内容管理数据等的区域。

[0149] 例如,通用区 52 是服务器和用户的记录和再现设备能自由写入数据且能从中自由读取数据的区域。

[0150] 另一方面,保护区 51 是不允许自由访问的区域。

[0151] 保护区 51 被分成作为多个分区的块(#0、#1、#2、…),在块单元中设置访问权。

[0152] 例如,当用户所用的记录和再现设备、经由网络连接的服务器等试图写入或读取数据时,存储卡 31 的数据处理单元基于预先存储在存储卡 31 中的程序根据每个设备确定是否能以块为单位执行读取或写入。

[0153] 存储卡 31 设置有用于执行预先存储的程序的数据处理单元和执行认证处理的认证处理单元,存储卡 31 首先对试图向存储卡 31 写入数据或从存储卡 31 读取数据的设备执行认证处理。

[0154] 在认证处理的步骤中,从对应的设备(即访问请求设备)中读取诸如公共密钥证书的设备证书。

[0155] 例如,当访问请求设备是服务器时,接收到由服务器所拥有的服务器证书,利用证书中描述的信息确定是否能够允许以保护区 51 的块(分区)为单位进行访问。

[0156] 另外,当访问请求设备是主机设备时,例如是作为记录和再现内容的用户装置的记录和再现设备(主机),接收到记录和再现设备(主机)所拥有的主机证书,并利用证书中描述的信息确定是否能允许对保护区 51 的各个块(分区)进行访问。

[0157] 以图 3 中所示的保护区 51 中的块(如图中所示的 #0、#1、#2…)为单位执行访问权确定处理。存储卡 31 使服务器或主机以块为单位执行允许的处理(用于读取 / 写入数据等的处理)。

[0158] 以试图访问内容的设备为单位,例如以内容服务器或记录和再现设备(主机)为单位设置介质读写的限制信息(PAD 读 /PAD 写)。信息被记录在主机证书或与各个设备相对应的服务器证书中。

[0159] 另外,“证书”在下面的说明中简称为“Cert (证书)”。

[0160] 如上所述,存储卡 31 基于预先存储在存储卡 31 中的预定程序验证记录在服务器证书或主机证书中的数据,并且执行仅允许访问访问允许区的 处理。

[0161] [3. 关于包含对保护区的访问允许的信息的证书]

[0162] 下面,将参照图 4 和图 5,说明在服务器或作为用户装置的主机装置(= 记录和再现设备)访问存储卡 31 中的上述保护区 51 时呈现给存储卡的证书的配置实例。

[0163] 如上所述,存储卡 31 对试图将数据写入存储卡 31 或从中读取数据的设备执行认

证处理。在认证处理步骤中，从相应的设备（即访问请求设备）中接收诸如公共密钥证书的设备证书（例如，服务器证书或主机证书），利用证书中描述的信息确定是否允许对保护区51中的各个分区进行访问。

[0164] 将参照图4，以存储在如图1B中所示的诸如记录和再现专用装置21、PC22、移动终端23等的用户装置（主机装置）上的主机证书的配置实例为例来说明在认证处理中使用的设备证书。

[0165] 例如，作为公共密钥证书发布方的认证站将主机证书提供给各个用户装置（主机装置）。例如，主机证书是用户装置的证书，该证书是认证站为允许内容使用处理的用户装置（主机装置）发布的，该证书中存储有公共密钥等。主机证书通过设置认证站的秘密密钥（secret key）的签名而配置为可防止伪造的数据。

[0166] 另外，例如基于关于设备类型的设备检验，当设备被制造时，可以在设备中的存储器上存储设备证书。如果在用户购买设备之后获得设备证书，则可应用如下配置：用于检验设备的类型、可用内容的类型等的处理基于设备与认证站或另一管理站之间的预定顺序来配置，并将证书发布给设备并且存储在设备的存储器上。

[0167] 另外，访问存储卡31中的保护区的服务器拥有服务器证书，其配置与主机证书的配置相同，其中记录有服务器公共密钥和存储卡访问允许信息。

[0168] 图4示出由认证站提供给各个主机装置（用户装置）的主机证书的具体实例。

[0169] 主机证书包括如图4所示的下列数据：(1)类型信息；(2)主机ID（用户装置ID)；(3)主机公共密钥；(4)保护区访问权信息（介质保护区的读写限制信息（PAD读/PAD写））；(5)其它信息；(6)签名。

[0170] 下文中，将说明数据(1)至(6)。

[0171] (1)类型信息

[0172] 类型信息是表示证书类型和用户装置类型的信息，例如，表示证书是主机证书的数据、表示诸如PC或音乐播放器的设备的类型的信息被记录在类型信息中。

[0173] (2)主机ID

[0174] 主机ID是记录作为装置标识信息的设备ID的区域。

[0175] (3)主机公共密钥

[0176] 主机公共密钥是主机装置的公共密钥。提供给主机装置（用户装置）的主机公共密钥和秘密密钥基于公共密钥加密方案配置密钥对。

[0177] (4)保护区访问权信息（介质中保护区的读写限制信息（PAD读/PAD写））

[0178] 在保护区访问权信息中，以保护区51中的块（分区）为单位设置在存储中的信息位于内容记录介质中，例如位于允许数据读写的图3所示的存储卡31中。

[0179] 访问权被记录为以保护区中的块（分区）为单位的访问权。

[0180] (5)其它信息，(6)签名

[0181] 各种信息与上述信息(1)至(4)一起记录在主机证书中，主机证书中还记录有用于信息(1)至(5)的签名。

[0182] 通过认证站的秘密密钥执行签名。当记录在主机证书中的信息（例如，主机公共密钥）被提取和使用时，首先通过应用认证站的公共密钥来执行签名验证处理，以确认主机证书上没有进行伪造，在已经进行确认的条件下使用诸如主机公共密钥的证书存储数据。

[0183] 图 4 示出主机证书，主机证书存储关于允许用户装置（主机装置）访问存储卡中的保护区的信息。以与图 4 所示的主机证书相同的方式设置存储卡中的保护区允许访问信息的证书（服务器证书，例如存储有服务器公共密钥的公共密钥证书）被提供给服务器，服务器访问保护区，服务器诸如是将内容提供给存储卡的内容提供服务器。

[0184] 将参照图 5，说明提供到服务器的服务器证书的配置实例。另外，下面说明中的服务器包括图 1A 中所示的所有的内容提供方，即将内容提供 给用户装置的诸如广播站 11 和内容服务器 12 的所有设备。

[0185] 例如通过作为公共密钥证书发布方的认证站将服务器证书提供给提供内容的内容服务器的设备等。例如，服务器证书是为认证站允许其执行内容提供处理的服务器发布的服务器证书，并且服务器证书是存储有服务器公共密钥等的证书。服务器证书通过设置认证站的秘密密钥的签名而被配置为防止伪造的数据。

[0186] 图 5 示出由认证站提供给各个内容服务器的服务器证书的具体实例。

[0187] 如图 5 所示，与参照图 4 描述的主机证书相似，服务器证书包括下列数据，即 :（1）类型信息、（2）服务器 ID、（3）服务器公共密钥、（4）介质读写限制信息（PAD 读 /PAD 写）、（5）其它信息，以及（6）签名。

[0188] 上述信息与上述参照图 4 所述的信息相同，省略其说明。

[0189] 另外，关于（4）介质读写限制信息（PAD 读 /PAD 写），以存储卡 31 中的保护区 51 中的块（分区）为单位的访问权（数据读写允许信息）被以服务器为单位记录。

[0190] 另外，当记录在服务器证书中的信息（例如服务器公共密钥）被提取和使用时，首先通过应用认证站的公共密钥执行签名验证处理，以确认服务器证书上没有进行伪造，诸如服务器公共密钥的证书存储数据在已经进行确认的条件下被使用。

[0191] [4. 关于通过应用每个设备的证书来访问存储卡的处理的实例]

[0192] 如上参照图 4 和图 5 所述，当服务器或主机装置（诸如记录和再现设备的用户装置）访问存储卡 31 中的保护区 51 的块时，需要将图 4 或图 5 所示的证书呈现给存储卡。

[0193] 存储卡检验图 4 或图 5 所示的证书，并确定是否可以以图 3 所示的存储卡 31 中的保护区 51 的块为单位允许访问。

[0194] 主机装置拥有例如上面参照图 4 描述的主机证书，且提供内容等的服务器拥有上面参照图 5 描述的服务器证书。

[0195] 当这些设备中的每一个设备访问存储卡中的保护区时，需要将各个设备拥有的证书呈现给存储卡，并且使存储卡基于验证确定是否允许访问。

[0196] 参照图 6，在请求访问存储卡的访问请求设备是服务器的情况和请求访问存储卡的访问请求设备是诸如记录和呈现设备的主机装置的情况下，对访问限制设置实例进行说明。

[0197] 在图 6 中，以从左到右的顺序示出了服务器 A61、服务器 B62、主机装置 63 和存储卡 70，服务器 A61、服务器 B62、主机装置 63 是存储卡的访问请求设备。

[0198] 服务器 A61 和服务器 B62 例如提供加密内容（Con1、Con2、Con3、…），作为记录在存储卡 70 中的内容。

[0199] 这些服务器还提供作为解码加密内容的密钥的标题密钥（Kt1、Kt2、…）以及使用规则（UR1、UR2、…）。

[0200] 主机装置 63 是执行用于再现存储在存储卡 70 上的内容的处理的装置。

[0201] 主机装置 63 读取记录在存储卡 70 的通用区 90 中的加密内容 Con1、Con2、Con3、…）和使用规则（UR1、UR2、…）。此外，主机装置 63 从保护区 80 的块（分区）81、82 中读取应用于内容解码处理的标题密钥（Kt1、Kt2、…），利用标题密钥执行解码处理，并且基于使用规则使用内容。

[0202] 存储卡 70 包括保护区 80 和通用区 90，并且加密内容、使用规则等被记录在通用区 90 中。

[0203] 作为用于再现内容所需的密钥的标题密钥被记录在保护区 80 中。

[0204] 如上面参照图 3 描述的，保护区 80 被划分为多个块（分区）。

[0205] 在图 6 的实例中，仅示出两个块，即块 #0（保护区 #0）81 和块 #1（保护区 #1）82。

[0206] 在保护区 80 中，设置其它多个块。

[0207] 可应用各种块设置状态。

[0208] 在图 6 所示的实例中，块 #0（保护区 #0）81 是仅用于服务器 A61 的块，即用于存储用于解码由服务器 A61 提供的内容的标题密钥的区域。

[0209] 块 #1（保护区 #1）82 是仅用于服务器 B62 的块，即用于存储用于解码由服务器 B62 提供的内容的标题密钥的区域。

[0210] 在这种设置中，提供内容的服务器 A61 在块 #0（保护区 #0）81 中记录用于解码提供的内容所需的标题密钥。

[0211] 在这种情况下，记录在服务器 A61 的服务器证书中的写入允许区信息（PAD 写）被构造为：设置允许在块 #0（保护区 #0）81 中进行写入的 证书。

[0212] 在图中所示实例中，也可以将允许读取设置在被设置为允许写入的块中。

[0213] 另外，服务器 B62 在块 #1（保护区 #1）82 中记录用于解码提供的内容所需的标题密钥。

[0214] 在这种情况下，记录在服务器 B62 的服务器证书中的写入允许区信息（PAD 写）被构造为：设置成允许在块 #1（保护区 #1）82 中进行写入的证书。

[0215] 另外，作为读取记录在块 #0 和 #1 中的标题密钥并且再现内容的再现设备的主机装置 63 所拥有的主机证书被配置为设置允许从块 #0 和 #1 读取的证书。

[0216] 在该实例中，主机证书不设置允许写入块 #0 和 #1。

[0217] 然而，进行设置使得可在删除内容时删除与删除内容对应的标题密钥，因此可对于删除处理设置允许写入。

[0218] 另外，当主机装置 63 在其它处理时需要在保护区写入数据时，可为主机证书设置允许写入。

[0219] 当从访问请求设备接收到访问保护区 80 的请求时（访问请求设备诸如是提供内容的服务器或使用内容的主机），存储卡 70 的数据处理单元参考各个设备的设备证书，确认以块为单位的访问允许信息，并且确定是否允许访问各个块。

[0220] 存储卡 70 根据来自访问请求设备的请求数据写入或数据读取的输入确定读写请求数据的类型，并且选择块（#0、#1、#2、…）作为在其中写入数据块或从其中读取数据的块。

[0221] 访问控制信息被记录在每个访问请求设备的如上参照图 4 和图 5 所述的证书（服

务器证书、主机证书等）中，存储卡首先对从访问请求设备接收到的证书进行签名验证，确认证书的有效性，然后读取证书中描述的访问控制信息，即下列信息：读取允许区信息（PAD 读）；及写入允许区信息（PAD 写）。

[0222] 存储卡基于上述信息仅允许并且执行对于访问请求设备允许的处理。

[0223] [5. 关于使用加密内容签名（ECS）发布方的内容提供系统]

[0224] 如上参照图 1A 至图 1C 所述，提供给用户装置的内容是从内容提供方提供的。然而，内容提供方自身在某些情况下可能传输不当复制内容。下文中，将说明还能防止除用户装置以外的配置的不当处理的配置，诸如服务器的不当处理。

[0225] 参照图7，将说明本公开的用于防止内容的不当使用的信息处理系统的整体构造。

[0226] 图 7 示出信息处理系统的整体构造实例。在图 7 中，以层级结构的形式示出四类设备：（A）许可发布方（LA）101；（B）加密内容签名（ECS）发布方 102-1 至 102-n；（C）内容提供方（内容服务器）103-1 至 103-m；以及（D）用户装置（内容再现设备）104-1 至 104-f。

[0227] 图 7 示出的（C）内容提供方（内容服务器）103-1 至 103-m 与图 1A 所示的广播站 11 和内容服务器 12 等对应。

[0228] 此外，图 7 示出的（D）用户装置（内容再现设备）104-1 至 104-f 与图 1B 所示的诸如记录和再现专用设备 21、PC22、移动终端 23 等的用户装置对应。

[0229] （C）内容提供方（内容服务器）103-1 至 103-m 包括各种信息处理设备，诸如内容服务器的在介质中发送内容或记录内容的设备、广播站或提供诸如存储有内容的盘的介质的介质提供公司。可以有多种内容提供方。

[0230] （D）用户装置（内容再现设备）104-1 至 104-f 是从内容提供方（内容服务器）103-1 至 103-m 经由互联网、广播站或诸如盘的介质接收或读取诸如电影或音乐或其它各种内容并且对内容执行再现处理的设备。具体地，包括各种信息处理设备，诸如能再现内容的 PC、移动终端、DVD 播放器、BD 播放器和电视。

[0231] （B）加密内容签名（ECS）发布方 102-1 至 102-n 产生与由（C）内容提供方（内容服务器）103-1 至 103-m 提供的内容相对应的加密内容签名文件（ECS 文件）。

[0232] 在将诸如电影内容的新内容提供给用户设备 104 时，例如，（C）内容提供方（内容服务器）103-1 至 103-m 请求加密内容签名（ECS）发布方 102 产生与内容相对应的加密内容签名文件（ECS 文件）。

[0233] （B）加密内容签名（ECS）发布方 102-1 至 102-n 响应于请求生成加密内容签名文件（ECS 文件），并且将加密签名内容文件（ECS 文件） 提供给（C）内容提供方（内容服务器）103。

[0234] 另外，稍后将详细说明加密内容签名文件（ECS 文件）的具体配置和生成处理。

[0235] （C）内容提供方（内容服务器）103 从（B）加密内容签名（ECS）发布方 102 接收加密内容签名文件（ECS 文件），并且将具有加密内容的加密内容签名文件（ECS 文件）提供给（D）用户装置（内容再现设备）104。

[0236] （D）用户装置（内容再现设备）104 在再现内容之前对加密内容签名文件（ECS 文件）执行签名验证处理，并且仅当确认已经成功进行签名验证处理时允许解码和再现内容。

[0237] 另外，用户装置（内容再现装置）104 在其上存储有基于用于在加密内容签名文件（ECS 文件）的签名验证的条件下执行解码和再现内容序列的再现处理程序，并且基于再现

处理程序执行用于确定内容是否能被再现的处理，诸如对加密内容签名文件（ECS 文件）执行的签名验证，并执行内容再现。

[0238] 例如，当未成功对加密内容签名文件（ECS 文件）执行签名验证时，则禁止内容的再现。

[0239] 许可发布方（LA）101 提供允许将 ECS 文件发布到加密内容签名（ECS）发布方 102 的许可。

[0240] 许可发布方（LA）101 基于预定的许可发布序列确认（B）加密内容签名（ECS）发布方 102-1 至 102-n 的有效性，并且当确认有效时，将许可发布给加密内容签名（ECS）发布方。

[0241] 另外，许可例如具体为具有许可发布方（LA）101 的秘密密钥的签名的公共密钥证书。在公共密钥证书上，存储有加密内容签名（ECS）发布方 102 的公共密钥。另外，（A）许可发布方（LA）101 还将与存储在公共密钥证书上的公共密钥相对应的秘密密钥提供给加密内容签名（ECS）发布方 102。

[0242] 接着，将参照附图 8，对（A）许可发布方（LA）101、（B）加密内容签名（ECS）发布方 102 和（C）内容提供方（内容服务器）103 执行的处理进行说明。

[0243] 图 8 是示出三个设备（即（A）许可发布方（LA）101、（B）加密内 容签名（ECS）发布方 102 和（C）内容提供方（内容服务器）103）及各个设备执行的代表性处理的图。

[0244] 由许可发布方（LA）101 执行的处理示出为（A1）和（A2）。

[0245] 许可发布方（LA）101 执行下列处理，即：处理（A1）和处理（A2）。在处理（A1）中，许可发布方（LA）101 将具有截止日期的 ECS 发布方证书提供给加密内容签名（ECS）发布方 102，在处理（A2）中，许可发布方（LA）101 将 ECS 发布方密钥撤销列表提供给内容提供方 103。

[0246] 由加密内容签名（ECS）发布方 102 执行的处理示出为处理（B1）和（B2）。

[0247] 加密内容签名（ECS）发布方 102 执行下列处理，即：处理（B1）和处理（B2）。在处理（B1）中，加密内容签名（ECS）发布方 102 生成加密内容证书文件（ECS 文件），在处理（B2）中，加密内容签名（ECS）发布方 102 将加密内容证书文件（ECS 文件）提供给内容提供方 103。

[0248] 由内容提供方 103 执行的处理示出为（C1）和（C2）。

[0249] 内容提供方 103 执行下列处理，即：处理（C1）和处理（C2）。在处理（C1）中，内容提供方 103 将用于生成 ECS 文件的数据（诸如内容哈希列表集、标题密钥的哈希值、块标识符等）提供给加密内容签名（ECS）发布方 102，在处理（C2）中，内容提供方 103 执行用于利用 ECS 文件来确定内容是否可被提供的处理。

[0250] [6. 关于 ECS 文件的配置实例]

[0251] 接着，将说明由加密内容签名（ECS）发布方 102 生成的 ECS 文件的配置实例。

[0252] 图 9A 和图 9B 示出还被设置为 ECS 文件的配置数据的 ECS 发布方证书的数据配置实例。

[0253] ECS 文件是由加密内容签名（ECS）发布方 102 生成的文件，该文件上存储有作为配置数据的从内容提供方 103 接收到的内容哈希列表集、标题密钥的哈希值、块标识符等。

[0254] 如图 9A 所示，ECS 文件包括下列数据：（1）内容哈希列表集；（2）ECS 发布日期；（3）块标识符（PAD 块编号）；（4）ECS 发布方的签名；（5）ECS 发布方证书；和（6）内容块表

(存储的内容块表)。

[0255] (1)内容哈希列表集是由内容提供方(内容服务器)103 生成的数 据和由加密内容签名(ECS)发布方 102 接收的数据。(1)内容哈希列表集是包括哈希值及其属性信息的数据,哈希值是基于内容配置数据生成的数据,内容配置数据是基于提供给用户设备的内容(具体地,诸如由用户设备再现的电影的内容)生成的,属性信息是关于表示作为哈希值的生成源的内容块的位置等的偏移、长度等的信息。

[0256] (2)ECS 发布日期是关于由加密内容签名(ECS)发布方 102 生成 ECS 文件的日期的信息。

[0257] 日期信息与生成(4)ECS 发布方签名的日期相对应。

[0258] (3)块标识符(PAD 块编号)是从内容提供方(内容服务器)103 传输到加密内容签名(ECS)发布方 102 的数据,并且是介质中的保护区的块标识符,该介质中存储有作为与由内容提供方 103 提供给用户装置 104 的内容相对应的加密密钥的标题密钥。(3)块标识符(PAD 块编号)是介质中的保护区的可被内容提供方 103 使用的块标识符。

[0259] (4)ECS 发布方签名(ECS 签名)

[0260] 如参照图 3 和图 6 等描述的,介质中的保护区中的可被内容提供方使用的块被预先设置,并且记录有访问允许块信息。

[0261] (4)ECS 发布方签名是 ECS 发布方的电子签名。

[0262] 作为签名的目标的数据是包括内容哈希列表集、ECS 发布日期、块标识符、标题密钥(哈希值)等的配置数据。

[0263] (5)ECS 发布方证书

[0264] (5)ECS 发布方证书是与 ECS 发布方 102 相对应的公共密钥证书,如图 9B 所示,其存储有 ECS 发布方 102 的公共密钥等。稍后将说明其配置。

[0265] (6)内容块表(存储的内容块表)

[0266] (6)内容块表(存储的内容块表)被设置为域(field),当与多个内容项对应的哈希列表被记录在内容哈希列表集中时,各个哈希列表和内容之间的对应信息被记录在该域中。

[0267] 接着,将说明图 9B 中所示的 ECS 发布方证书的数据配置。

[0268] ECS 发布方证书由许可发布方(LA)101 生成并且提供给 ECS 发布方 102。ECS 发布方 102 将用于生成 ECS 发布方证书所需的数据提供给 许可发布方(LA)101,并且请求生成 ECS 发布方证书。

[0269] 许可发布方(LA)101 响应于请求生成 ECS 发布方证书。

[0270] 如图 9B 所示,ECS 发布方证书是包括下列数据的文件 :(1)ECS 证书 ID、(2)块标识符开始编号(开始 PAD 块编号)、(3)块标识符范围(PAD 块编号计数器)、(4)发布方证书截止日期、(5)ECS 发布方公共密钥,以及(6)LA 签名。

[0271] (1)ECS 证书 ID 是 ECS 证书的标识。

[0272] (2)块标识符开始编号(开始 PAD 块编号)是介质中的保护区中的 ECS 发布方 102 可允许内容提供方 103 进行访问的访问允许块的开始编号。

[0273] (3)块标识符范围(PAD 块编号计数器)是表示介质中的保护区中的 ECS 发布方 102 可允许内容提供方 103 进行访问的从访问允许块的开始编号起的范围的信息。

[0274] (4)发布方证书截止日期是关于发布方证书截止日期的信息。

[0275] (5)ECS 发布方公共密钥是 ECS 发布方的公共密钥。

[0276] (6)LA 签名是图 7 和图 8 所示的许可发布方(LA)的电子签名。(6)LA 签名是基于 ECS 发布方证书的上面的配置数据(1)至(5)生成的电子签名。

[0277] 图 10 是示出 ECS 文件的语法(syntax)的图,图 11 是示出 ECS 发布方证书的语法的图。

[0278] 另外,记录在 ECS 发布方证书中的两个数据项(即(2)块标识符开始编号(开始 PAD 块编号)和(3)块标识符范围(PAD 块编号计数器))是表示介质中的保护区中的 ECS 发布方 102 可允许内容提供方 103 进行访问的访问允许块的信息。

[0279] 具体地,该信息等同于将满足块标识符开始编号≤ N ≤块标识符开始编号 + 块标识符范围的所有的 N 设置为块标识符。

[0280] 另外,块标识符开始编号 =0×FFFFFFFF 的设置表示介质中的保护区中所有块都是访问允许块。

[0281] 尽管上述说明是在参照图 9 至图 11 所述的实例中以 ECS 文件包括 ECS 发布方证书的配置进行说明的,但是 ECS 文件不包括 ECS 发布方证 书的其它配置也适用,ECS 文件和 ECS 发布方证书可配置为独立文件。

[0282] [7、关于 ECS 发布方证书撤销列表的配置]

[0283] 接着,将参照图 12 说明 ECS 发布方证书撤销列表的配置。

[0284] ECS 发布方证书撤销列表(ECS 发布方密钥撤销列表)是如上参照图 8 所述的许可发布方(LA) 101 所发布的列表。该列表例如被内容提供方 103 使用。

[0285] 许可发布方(LA)101 使得已经确定为不当的存储有 ECS 发布方的公共密钥的 ECS 发布方证书(见图 9B)失效,并且生成 ECS 发布方证书撤销列表,作为登记有失效的 ECS 发布方(具体地,ECS 发布方证书)的标识符(ID)的列表。

[0286] 如图 12 所示,ECS 发布方证书撤销列表在其上存储下列数据。即 :(1)版本、(2)登入数目、(3)撤销(无效)的 ECS 发布方证书的 ID、(4)撤销的 ECS 发布方证书的撤销时期,和(5)许可发布方(LA) 101 的电子签名。

[0287] (5)许可发布方(LA) 101 的电子签名是对数据(1)至(4)的签名。

[0288] 另外,当新发现不当 ECS 发布方时,ECS 发布方的 ID 被添加到 ECS 发布方撤销列表,连续地发布更新的新版本的列表,并且将该列表提供给内容提供方 103。

[0289] [8. 关于用于生成加密内容签名文件(ECS 文件)的处理]

[0290] 接着,将参照图 13 说明用于生成加密内容签名文件(ECS 文件)的处理。

[0291] 加密内容签名(ECS)发布方 102 基于来自内容提供方(内容服务器) 103 的生成请求而生成加密内容签名文件(ECS 文件)。

[0292] 当内容提供方(内容服务器) 103 向用户装置 104 提供诸如电影内容等的新内容时,内容提供方(内容服务器) 103 请求生成到与加密内容签名(ECS)发布方 102 的内容相对应的加密内容签名文件(ECS 文件)。

[0293] 加密内容签名(ECS)发布方 102 响应于请求生成加密内容签名文件(ECS 文件),并将加密内容签名文件(ECS 文件)提供给内容提供方(内容服务器) 103。

[0294] 图 13 是例示由内容提供方(内容服务器)103 和加密内容签名(ECS)发布方 102 在

用于生成加密内容签名文件(ECS 文件)的处理中所执行的处理。

[0295] 在请求生成新的加密内容签名文件(ECS 文件)时,内容提供方(内容服务器)103 生成内容哈希列表集183,内容哈希列表集包括基于如图13所示的内容181的配置数据(内容块)生成的哈希值。

[0296] 另外,内容哈希列表集 183 被生成为存储基于提供给用户装置 104 的加密内容的配置数据(内容块)生成的哈希值的内容哈希列表集。

[0297] 内容提供方(内容服务器)103 将生成的内容哈希列表集 183 提供给加密内容签名(ECS)发布方 102。

[0298] 此外,内容提供方(内容服务器)103 还将作为将应用于加密内容 181 的加密密钥的标题密钥 182 或标题密钥的哈希值提供给加密内容签名(ECS)发布方 102。

[0299] 内容哈希列表集 183 是包括哈希值及其属性信息的数据,哈希值是基于内容配置数据生成的,内容配置数据是基于提供给用户装置的内容生成的。

[0300] 另外,属性信息例如包括已经计算出哈希值的内容块的位置信息。

[0301] 在图13所示的步骤S11中,加密内容签名(ECS)发布方102为从内容提供方(内容服务器)103 接收的数据和 ECS 文件的配置数据生成签名,数据具体地为内容哈希列表集、ECS 发布日期、块标识符和标题密钥(哈希)。

[0302] 在生成签名数据时,通过应用由加密内容签名(ECS)发布方 102 拥有的秘密密钥来生成签名。例如,基于 ECDSA 算法生成签名。

[0303] 如图 13 所示,生成的签名被设置为加密内容签名文件(ECS 文件)的配置数据。

[0304] 如上面参照图 9A 和图 9B 描述的,由加密内容签名(ECS)发布方 102 生成的加密内容签名文件(ECS 文件)200 包括下列数据作为配置数据。也就是,加密内容签名文件(ECS 文件)是包括如下数据的文件:(1)内容哈希列表集、(2)ECS 发布日期、(3)块标识符(PAD 块编号)、(4)ECS 发布方的签名、(5)ECS 发布方证书,和(6)内容块表(存储的内容块表)。

[0305] [9、关于通过应用 ECS 文件和 ECS 发布方证书中的日期信息进行的处理]

[0306] 接着,将对通过应用 ECS 文件和 ECS 发布方证书中的日期信息进行的处理进行说明。

[0307] 如上面参照图 9A 和图 9B 描述的,各种日期信息被记录在(1)将被提供给内容提供方的 ECS 发布方 102 所生成的 ECS 文件中和(2)将被提供给 ECS 发布方 102 的许可发布方(LA)101 生成的 ECS 发布方证书中。

[0308] 例如,ECS 发布日期被记录在 ECS 文件中。

[0309] 另外,发布方证书截止日期被记录在 ECS 发布方证书中。

[0310] 内容提供方 103 通过应用记录在 ECS 文件和 ECS 发布方证书中的日期信息和上面参照图 12 所述的 ECS 发布方证书撤销列表,来执行用于确定内容是否可以被提供给用户装置 104 的处理。

[0311] 另外,从内容提供方 103 接收内容的用户装置也通过应用记录在 ECS 文件和 ECS 发布方证书中的日期信息和上面参照图 12 描述的 ECS 发布方证书撤销列表,来执行用于确定用户装置 104 是否可再现该内容的处理。

[0312] 下文中,将描述该处理。

[0313] 首先,将参照图 14 和图 15 所示的序列图来说明用于生成加密内容签名文件(ECS

文件）并提供和使用内容的处理序列。

[0314] 图 14 从左侧起按顺序示出许可发布方 101、加密内容签名（ECS）发布方 102 以及内容提供方 103，步骤 S111 和 S121 至 S128 中的处理示出为时间序列处理。

[0315] 将说明处理步骤。

[0316] 步骤 S111

[0317] 步骤 S111 是许可发布方 101 为加密内容签名（ECS）发布方 102 发布许可（ECS 发布方证书）的处理。

[0318] 如上参照图 8 等所述的，许可发布方 101 将作为许可发布 ECS 文件（即 ECS 发布方证书）的许可提供给加密内容签名（ECS）发布方 102。

[0319] 许可发布方（LA）101 基于预定的许可发布序列确认加密内容签名 （ECS）发布方 102 的有效性，当确认有效时，将 ECS 发布方证书发布给加密内容签名（ECS）发布方。

[0320] ECS 发布方证书是具有如上参照图 9B 描述的数据配置的公共密钥证书。ECS 发布方证书在其上存储有加密内容签名（ECS）发布方 102 的公共密钥。另外，（A）许可发布方（LA）101 还将与在 ECS 发布方证书上存储的公共密钥相对应的秘密密钥提供给加密内容签名（ECS）发布方。

[0321] 步骤 S121 至 S124 是用于生成如上参照图 13 描述的加密内容签名文件（ECS 文件）的处理的序列。

[0322] 根据提供的内容顺次执行处理，从而使得内容提供方 103 在将新内容提供给用户装置时获取与新内容相对应的加密内容签名文件（ECS 文件）。

[0323] 处理是在加密内容签名（ECS）发布方 102 和内容提供方 103 之间执行的。

[0324] 首先，在步骤 S121 中，内容提供方 103 生成用于生成加密内容签名文件（ECS 文件）所需的数据。

[0325] 具体地，执行用于生成如上参照图 13 描述的内容哈希列表集 183 的处理。

[0326] 如上所述，内容哈希列表集是包括哈希值及其属性信息的数据，哈希值是基于内容配置数据生成的，内容配置数据是基于提供给用户装置的内容生成的，提供给用户装置的内容具体为诸如电影的由用户装置再现的内容。

[0327] 属性信息例如包括已经计算出哈希值的内容块的位置的信息。

[0328] 另外，内容提供方 103 还生成要应用到内容加密和解码处理的标题密钥和将作为数据提供给加密内容签名（ECS）发布方 102 的标题密钥的哈希值。

[0329] 接着，在步骤 S122 中，内容提供方 103 将生成的数据发送到加密内容签名（ECS）发布方 102，并且请求生成和发送加密内容签名文件（ECS 文件）。

[0330] 接着，在步骤 S123 中，加密内容签名（ECS）发布方 102 对从内容提供方 103 接收的数据执行生成签名的处理。

[0331] 也就是，执行在如上参照图 13 描述的步骤 S11 中的用于生成签名的处理。

[0332] 此外，生成具有如上参照图 9A 描述的数据配置的加密内容签名文件（ECS 文件），在步骤 S124 中，加密内容签名文件（ECS 文件）被发送到内容提供方 103。

[0333] 如上参照图 9A 描述的，加密内容签名文件（ECS 文件）包括以下数据：（1）内容哈希列表集、（2）ECS 发布日期、（3）块标识符（PAD 块编号）、（4）ECS 发布方的签名、（5）ECS 发布方证书，及（6）内容块表（存储的内容块表）。

[0334] 内容提供方103接收加密内容签名文件(ECS文件),在步骤S125中,执行用于确定内容是否能被提供的处理,以便确定是否允许提供已经应用加密内容签名文件(ECS文件)的内容。

[0335] 当在步骤S126中确定允许提供内容时,在步骤S127中执行用于将内容提供给用户装置的处理。

[0336] 当在步骤S126中确定不允许提供内容时,处理进行到步骤S128,停止用于提供内容的处理。

[0337] 另外,稍后将参照图16和后继附图将详细说明步骤S125至S128中的处理。

[0338] 接着,将参照图15说明用于将内容从内容提供方103提供给用户装置104并且用于由用户装置104再现内容的序列。

[0339] 图15以从左侧起按顺序示出了内容提供方103和用户装置104。

[0340] 首先,在步骤S131中,内容提供方103向用户装置发送如下数据:(1)加密内容、(2)加密内容签名文件(ECS文件),及(3)标题密钥。

[0341] 假定用户装置104已经请求内容提供方103传送内容,该请求作为步骤S131中的处理的预处理。内容提供方103根据来自用户装置的请求提供内容。

[0342] 另外,由内容提供方103在步骤S131中发送的(1)加密内容是利用与内容对应设置的(3)“标题密钥”加密的内容。

[0343] 另外,(2)加密内容签名文件(ECS文件)是与上述(1)加密内容相对应地生成的文件,其上存储有如上参照图9A和图9B描述的加密内容签名文件(ECS文件)的配置数据。

[0344] 用户装置104接收数据并且将数据存储在诸如硬盘的介质上。

[0345] 此后,在执行用于再现内容的处理时,执行图15所示的步骤S132及后续步骤中的处理。

[0346] 在步骤S132中,用户装置104读取与将再现的内容相对应的加密内容签名文件(ECS文件),并且通过应用加密内容签名文件(ECS文件)来执行用于确定内容是否可被再现的处理,以便确定是否允许内容的再现。

[0347] 当在步骤S133中确定允许内容再现时,在步骤S134中执行用于再现内容的处理。

[0348] 当在步骤S133中确定不允许内容再现时,处理进行到步骤S135,停止用于再现内容的处理。

[0349] 稍后将参照图18详细说明步骤S132至S135的处理。

[0350] 接着,将参照图16和图17所示的流程图说明如上参照图14描述的由内容提供方执行的步骤S125至S128中的处理的详细序列,即用于通过应用加密内容签名文件(ECS文件)来确定内容是否可被提供的处理。

[0351] 作为图16所示的流程图中的步骤S151的预处理,内容提供方通过应用设置在从加密内容签名文件(ECS文件)发布方接收到的加密内容签名文件(ECS文件)中的ECS发布方签名来执行签名验证。

[0352] 当成功进行签名验证并且确认加密内容签名文件(ECS文件)有效时,内容提供方还对存储在加密内容签名文件(ECS文件)上的ECS发布方证书执行签名验证。在对两种签名验证成功完成的条件下,执行步骤S151及后续步骤中的处理。

[0353] 当上述两种签名验证中的至少之一未成功进行时,未确认加密内容签名文件(ECS

文件）的有效性或 ECS 发布方证书的有效性，因此，不执行步骤 S151 及后续步骤中的处理。在该情况下，也不执行用于提供内容的处理。

[0354] 当对加密内容签名文件（ECS 文件）和 ECS 发布方证书的两种签名验证成功完成时，确认加密内容签名文件（ECS 文件）的有效性和 ECS 发布方证书的有效性，内容提供方执行步骤 S151 中的处理。

[0355] 内容提供方读取作为记录在加密内容签名文件（ECS 文件）中的数据的 ECS 发布日期。此外，内容提供方读取作为记录在 ECS 发布方证书中的数据的 ECS 发布方证书截止日期。

[0356] 此外，内容提供方比较数据信息并且确定 ECS 发布方证书截止日期是否在 ECS 发布日期之前。

[0357] 如果 ECS 发布方证书截止日期在 ECS 发布日期之前（是），则内容提供方执行步骤 S156，并且停止加密内容的分发。

[0358] 如果 ECS 发布方证书截止日期不在 ECS 发布日期之前（否），则内容提供方执行步骤 S152，并且在步骤 S153 和后续步骤中启动通过应用记录在加密内容签名文件（ECS 文件）和 ECS 发布方证书中的时间信息（时间戳）确定内容是否可被提供的处理。

[0359] 在步骤 S153 中，内容提供方将 ECS 发布方证书截止日期与内容提供方所拥有的时钟或从可靠时间信息提供服务器获取的实际时间进行比较。

[0360] 如果 ECS 发布方证书截止日期在实际时间之前 1 天或更多天，则内容提供方执行步骤 S156 并且停止用于提供内容的处理。

[0361] 另一方面，如果 ECS 发布方证书截止日期不在实际时间之前 1 天或更多天，则处理进行到步骤 S154。

[0362] 在步骤 S154 中，内容提供方将 ECS 发布日期与内容提供方所拥有的时钟或从可靠时间信息提供服务器获取的实际时间进行比较。

[0363] 如果 ECS 发布日期在实际时间之前 1 天或更多天，则内容提供方执行步骤 S156 并且停止用于提供内容的处理。

[0364] 另一方面，如果 ECS 发布日期不在实际时间之前 1 天或更多天，则处理进行到步骤 S155。

[0365] 接着，将参照图 17 所示的流程图说明在步骤 S155 及后续步骤中执行的用于通过应用撤销列表确定内容是否可被提供的处理。

[0366] 另外，假定内容提供方已经预先获得如上参照图 12 描述的 ECS 发布方公共密钥撤销列表。例如，可从许可发布方（LA）101 获取 ECS 发布方公共密钥撤销列表。

[0367] 在步骤 S161 中，内容提供方从 ECS 发布方证书获取 ECS 证书标识符，并且确定标识符（ID）是否被登记在 ECS 发布方公共密钥撤销列表中。

[0368] 当标识符未被登记在 ECS 发布方公共密钥撤销列表中时（否），确认 ECS 发布方证书未被无效（撤销）并且仍有效，在这种情况下，内容提供方移动到步骤 S164 并且执行用于提供内容的处理。

[0369] 另一方面，在步骤 S161 中，确定 ECS 证书标识符（ID）被登记在 ECS 发布方公共密钥撤销列表中时（是），处理进行到步骤 S162。

[0370] 在步骤 S162 中，比较与两个日期有关的数据项，也就是，一个日期是被登记在 ECS

发布方公共密钥撤销列表中的ECS发布方证书失效(撤销)的日期,即撤销日期,另一日期是作为记录在加密内容签名文件(ECS 文件)中的数据的ECS发布日期。

[0371] 当作为记录在加密内容签名文件(ECS 文件)中的数据的ECS发布日期在撤销日期之前时(是),内容提供方移动到步骤S164,并且执行用于提供内容的处理。

[0372] 这是因为能够确定处理基于撤销之前的得当的ECS发布方证书。

[0373] 另一方面,当在步骤S162中作为记录在加密内容签名文件(ECS 文件)中的数据的ECS发布日期不在撤销日期之前时(否),内容提供方移动到步骤S163并停止用于提供内容的处理。

[0374] 这是因为能够确定处理基于撤销之后的不当ECS发布方证书。

[0375] 接着,将参照图18所示的流程图说明用于通过如上参照图15的步骤S132至S135描述的在内容装置104中应用加密内容签名文件(ECS 文件)确定是否允许内容再现的处理。

[0376] 在图18所示的步骤S171之前,用户装置通过应用设置在从内容提供方接收的加密内容签名文件(ECS 文件)中的ECS发布方签名来执行签名验证。

[0377] 当成功进行签名验证并且确认加密内容签名文件(ECS 文件)的有效性时,用户装置还对存储在加密内容签名文件(ECS 文件)上的ECS发布方证书执行签名验证。在对两种签名验证成功完成的条件下,执行步骤S171及后续步骤的处理。

[0378] 当上述两种签名验证中的至少之一未成功进行时,未确认加密内容签名文件(ECS 文件)的有效性或ECS发布方证书的有效性,因此,不执行步骤S171及后续步骤中的处理。在该情况下,也不执行用于再现内容的处理。

[0379] 当对加密内容签名文件(ECS 文件)和ECS发布方证书的两种签名验证成功完成时,确认加密内容签名文件(ECS 文件)的有效性和ECS发布方证书的有效性,用户装置执行步骤S171中的处理。

[0380] 在步骤S171中,用户装置读取作为记录在加密内容签名文件(ECS 文件)中的数据的ECS发布日期。

[0381] 此外,用户装置读取作为记录在ECS发布方证书中的数据的ECS发布方证书截止日期。

[0382] 此外,用户装置比较日期信息项并且确定ECS发布方证书截止日期是否在ECS发布日期之前。

[0383] 当ECS发布方证书截止日期在ECS发布日期之前时(是),处理执行步骤S175,并且不执行用于解码和再现内容的处理。

[0384] 这是因为,ECS发布方证书被确认是到期的ECS发布方证书。

[0385] 另一方面,当在步骤S171中ECS发布方证书截止日期不在ECS发布日期之前时(否),处理进行到步骤S172,并且在步骤S173和后续步骤中执行用于通过应用撤销列表确定内容是否可被提供的处理。

[0386] 另外,假定用户装置预先获得如上参照图12描述的ECS发布方公共密钥撤销列表。例如,用户装置可从许可发布方(LA)101获取ECS发布方公共密钥撤销列表。

[0387] 在步骤S173中,用户装置从ECS发布方证书获取ECS证书标识符并且确定该标识符(ID)是否被登记在ECS发布方公共密钥撤销列表中。

[0388] 当标识符未被登记时(否),确认ECS发布方证书未被无效(撤销)并且仍有效,在这种情况下,用户装置移动到步骤S176并且执行用于再现内容的处理。

[0389] 在启动用于再现内容的处理之前,执行用于获取和生成要应用于加密内容的解码的标题密钥的处理,以及用于通过应用包括在加密内容签名文件中的内容哈希列表进行交叉校验哈希值的处理。当成功进行交叉校验,并确认内容中没有进行伪造时,允许再现内容。

[0390] 另一方面,当在步骤S173中确定ECS证书标识符(ID)被登记在ECS发布方公共密钥撤销列表中时(是),处理执行步骤S174。

[0391] 在步骤S174中,比较与日期有关的两个数据项,也就是,一个日期是被登记在ECS发布方公共密钥撤销列表中的ECS发布方证书失效(撤销)的日期,即撤销日期,另一日期是作为记录在加密内容签名文件(ECS文件)中的数据的ECS发布日期。

[0392] 当作为记录在加密内容签名文件(ECS文件)中的数据的ECS发布 日期在撤销日期之前时(是),处理进行到步骤S176,并且执行用于再现内容的处理。

[0393] 这是因为能确定处理是基于撤销之前的得当ECS发布方证书的。

[0394] 另一方面,当在步骤S173中作为记录在加密内容签名文件(ECS文件)中的数据的ECS发布日期不在撤销日期之前时(否),处理进行到步骤S175,并停止用于再现内容的处理。

[0395] 这是因为能确定处理是基于撤销之后的不当ECS发布方证书的。

[0396] [10.关于关联加密密钥和ECS发布方签名的配置]

[0397] 接着,将说明关联加密密钥和ECS发布方签名的配置。

[0398] 如上参照图3和图6所述,用户装置104记录并且使用存储卡中的内容等,存储卡例如由快擦写存储器配置。

[0399] 如参照图3描述的,存储卡31中的存储区被配置成两个区域,即(a)保护区51和(b)通用区52。

[0400] (b)通用区52是由用户使用的记录和再现设备可访问的区域,其中记录有内容、与内容对应的使用规则、其它一般内容管理数据等。

[0401] 通用区52是服务器或用户的记录和再现设备可自由读写数据的区域。

[0402] 另一方面,(a)保护区51是不允许自由访问的区域。

[0403] 保护区51被划分为作为分区的多个块(#0、#1、#2、…),访问权被以块为单位设置。

[0404] 例如,当由用户使用的记录和再现设备或经由网络连接的服务器试图读写数据时,存储卡31的数据处理单元基于预先存储在存储卡31上的程序对每个设备以块为单位确定是否能进行读写。

[0405] 存储卡31设置有用于执行预先存储的程序的数据处理单元和用于执行认证处理的认证处理单元,并且对试图将数据写入存储卡31或从其读取数据的设备进行认证处理。

[0406] 在认证处理的步骤中,从对应的设备(即访问请求设备)接收诸如公共密钥证书的设备证书。

[0407] 例如,当访问请求设备是服务器时,接收到如上参照图5描述的服务器所拥有的服务器证书,并且利用证书描述的信息以保护区51中的块(分 区)为单位确定是否允许访

问。

[0408] 另外，当访问请求设备是主机装置(例如是作为记录和再现内容的用户装置的记录和再现设备(主机))时，接收到如上参照图 4 描述的记录和再现设备(主机)所拥有的主机证书，并且利用证书中描述的信息确定是否允许访问保护区 51 中的每个块(分区)。

[0409] 以图 3 中所示的保护区 51 中的块(#0、#1、#2、…)为单位执行用于确定访问权的处理。存储卡 31 使服务器或主机仅以块为单位执行允许的处理(数据读写处理等)。

[0410] 将参照图 19 说明当介质被安装在用户装置 104 上以记录从内容提供方 103 接收的内容时的数据记录配置实例。

[0411] 图 19 示出作为内容提供方的服务器 A201 将加密内容提供给安装在作为用户装置的主机 202 上的存储卡 210 并且在其中记录加密内容的处理实例。

[0412] 存储卡 210 包括保护区 211 和通用区 212。

[0413] 在执行用于提供加密内容的处理时，作为内容提供方的服务器 A201 在保护区的预定块中记录要应用于加密和解码提供的内容的标题密钥。

[0414] 服务器 A201 拥有上面参照图 5 描述的服务器证书。

[0415] 首先，服务器 A201 执行处理，以相互认证存储卡 210。在该情况下，服务器证书被输出到存储卡 210。

[0416] 存储卡 210 确认记录在从服务器 A201 接收到的服务器证书中的保护区访问权信息。

[0417] 只有当在确认处理中确定服务器 A201 具有对块 #0 的访问权(写入权)时，服务器 A201 才可以对设置在存储卡 210 的保护区 211 中的块 #0 写入数据。

[0418] 如附图所示，服务器 A201 存储有要应用到保护区 211 中的块 #0 (211) 上的提供内容的解码的标题密钥。

[0419] 另外，标题密钥本身并不原样存储在保护区上，而是(a)使用规则和(b)作为如上参照图 9A 和图 9B 描述的 ECS 文件的配置数据的 ECS 发布方签名的耦合数据的哈希值与标题密钥 Kt 之间的异或被记录在保护区上。

[0420] 例如，内容(a1)的标题密钥 Kt (a1) 在保护区上存储为下列标题密钥转换数据：Kt(a1)(+)(UR(a1)||ECSSig(a1))hash，其中，UR(a1) 表示与内容 a1 相对应的使用规则，ECSSig(a1) 表示作为与内容 a1 相对应的 ECS 文件的配置数据的 ECS 发布方的签名。

[0421] 另外，各个作为运算符的符号的含义如下：即，(+) 表示异或，|| 表示数据耦合(coupling)，a ||b 意味着数据 a 和数据 b 的耦合数据。“hash”意思是哈希值，“(a||b)hash”意思是数据 a 和数据 b 的耦合数据的哈希值。

[0422] 在图 19 的实例中，服务器 A 在存储卡中的通用区 212 中记录下列的内容：使用规则和 ECS 文件。

[0423] 即，记录内容集合 Con (a1)、Con (a2) 和 Con (a3)，与上述内容对应的使用规则 UR (a1)、UR (a2) 和 UR (a3)，以及与上述内容对应的 ECS 文件 ECS (a1)、ECS (a2) 和 ECS (a31)。

[0424] 此外，服务器 A 在存储卡中的保护区 211 中的块 #0 (221) 中记录下列数据。

[0425] 也就是，在其中记录有与内容相对应的标题密钥和耦合数据的哈希值之间的异或(XOR)结果，耦合数据是与内容相对应的使用规则和 ECS 发布方签名之间的耦合数据，也就

是：

[0426] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0427] Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

[0428] Kt(a3)(+)(UR(a3)||ECSSig(a3))hash

[0429] 虽然图 19 示出由服务器 A201 进行的处理实例，另一服务器 B 在保护区的被允许作为用于存储与由服务器 B 提供的内容（bx）相对应的标题密钥的区域的预定块上（例如块 #1）存储相同标题密钥转换数据，例如由服务器 B 提供的内容的 Kt(bx)(+)(UR(bx)||ECSSig(bx))hash 数据。

[0430] 图 20 示出使用内容的用户装置（主机）202 和上面存储有内容等的存储卡 210。

[0431] 用户装置（主机）202 拥有参照图 4 描述的主机证书。

[0432] 首先，用户装置（主机）202 执行用于相互认证存储卡 210 的处理。在该情况下，用户装置（主机）202 将主机证书输出到存储卡 210。

[0433] 存储卡 210 确认记录在从用户装置（主机）202 接收到的主机证书中 的保护区访问权信息。

[0434] 只有当在确认处理中确定用户装置（主机）202 拥有对块 #0 的访问权时，用户装置（主机）202 可以从设置在存储卡 210 的保护区 211 的块 #0 中读取数据。

[0435] 在相互认证和访问权确认之后，用户装置（主机）202 执行下列处理以使用内容。

[0436] 首先，用户装置（主机）202 从存储卡中的通用区 212 获取将使用的内容 Con（xy）、对应的使用规则 UR（xy）和 ECS 文件 ECS（xy）。

[0437] 接着，参照使用规则 UR（xy），确认保护区中的存储内容 Con（xy）的标题密钥的所在块。

[0438] 要使用内容 Con（xy）的块的标识符被记录在使用规则 UR（xy）中。

[0439] 当指定保护区 211 中存储标题密钥的块时，执行用于读取块中记录的数据的处理。

[0440] 例如，从选定的块中读取下列数据：Kt(xy)(+)(UR(xy)||ECSSig(xy))hash。

[0441] 接着，执行用于耦合从通用区 212 读取的使用规则 UR（xy）和存储在 ECS 文件 ECS（xy）上的 ECS 发布方签名（xy）的处理，并且执行用于计算哈希值的处理。

[0442] 也就是，计算出 (UR(xy)||ECSSig(xy))hash。

[0443] 计算结果被表示为 P（xy）。

[0444] 此后，通过执行下列计算获取标题密钥 Kt（xy）：

[0445] [从块读取的数据（标题密钥转换数据）](+)P(xy)

[0446] =(Kt(xy)(+)(UR(xy)||ECSSig(xy))hash)(+)P(xy)

[0447] =(Kt(xy)(+)(UR(xy)||ECSSig(xy))hash)(+)(UR(xy)||ECSSig(xy))hash)

[0448] =Kt(xy)

[0449] 通过计算处理获取标题密钥 Kt(xy)，利用获取的标题密钥解码并使用加密内容。

[0450] 将参照图 21 说明存储卡中记录的数据的实例。

[0451] 图 21 示出通过两个不同的服务器（即服务器 A 和服务器 B）写入存储卡中数据的实例。

[0452] 服务器 A 拥有存储卡中的保护区块 #0 的访问权。

[0453] 服务器 B 拥有存储卡中的保护区块 #1 的访问权。

[0454] 每个服务器均在安装在作为用户装置的主机装置上的存储卡中记录数据以及内容。

[0455] 由服务器 A 提供的内容假定为 Con（a1）、Con（a2）和 Con（a3）。

[0456] 由服务器 B 提供的内容假定为 Con（b1）和 Con（b2）。

[0457] 如图 21 中所示，服务器 A 在存储卡的通用区中记录下列数据：内容 Con（a1）、Con（a2）和 Con（a3），与上述内容相对应的使用规则 UR（a1）、UR（a2）和 UR（a3），以及与上述内容相对应的 ECS 文件 ECS（a1）、ECS（a2）和 ECS（a31）。

[0458] 此外，服务器 A 在存储卡的保护区中的块 #0 中记录下列数据。

[0459] 也就是，在其中记录要应用于内容的解码的标题密钥 Kt（a1）、Kt（a2）和 Kt（a3）的转换数据的数据，以及

[0460] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0461] Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

[0462] Kt(a3)(+)(UR(a3)||ECSSig(a3))hash。

[0463] 另一方面，服务器 B 在存储卡的通用区中记录下列数据：内容 Con（b1）和 Con（b2），与上述内容相对应的使用规则 UR（b1）和 UR（b2），以及与上述内容相对应的 ECS 文件 ECS（b1）和 ECS（b2）。

[0464] 此外，服务器 B 在存储卡的保护区中的块 #1 中记录下列数据。

[0465] 也就是，记录要应用于内容的解码的标题密钥 Kt（b1）和 Kt（b2）的转换数据的数据，以及

[0466] Kt(b1)(+)(UR(b1)||ECSSig(b1))hash

[0467] Kt(b2)(+)(UR(b2)||ECSSig(b2))hash。

[0468] 当各个服务器在存储卡的保护区的块中记录数据时，存储卡基于服务器证书中的上述记录确认访问权并且确认在块中写入数据的权利，仅当确认了访问权时，才执行数据写入。

[0469] 图 22 示出当服务器 A 和服务器 B 拥有存储卡中的保护区中的块 #0 的访问权，服务器 C 和服务器 D 拥有存储卡中的保护区中的块 #1 的访问权时，记录数据的实例。

[0470] 服务器 A 在存储卡的通用区中记录下列数据：内容 Con（a1）、Con（a2）和 Con（a3），与上述内容相对应的使用规则 UR（a1）、UR（a2）和 UR（a3），以及与上述内容相对应的 ECS 文件 ECS（a1）、ECS（a2）和 ECS（a31）。

[0471] 此外，服务器 A 在存储卡的保护区中的块 #0 中记录下列数据。

[0472] 也就是，在其中记录要应用于内容的解码的标题密钥 Kt（a1）、Kt（a2）和 Kt（a3）的转换数据的数据，以及

[0473] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash

[0474] Kt(a2)(+)(UR(a2)||ECSSig(a2))hash

[0475] Kt(a3)(+)(UR(a3)||ECSSig(a3))hash。

[0476] 服务器 B 在存储卡的通用区中记录下列数据：内容 Con（b1）和 Con（b2），与上述内容相对应的使用规则 UR（b1）和 UR（b2），以及与上述内容相对应的 ECS 文件 ECS（b1）和 ECS（b2）。

[0477] 此外，服务器 B 在存储卡的保护区中的块 #0 中记录下列数据。

[0478] 也就是，在其中记录要应用于内容的解码的标题密钥 Kt（b1）和 Kt（b2）的转换数据的数据，以及

[0479] Kt(b1)(+)(UR(b1)||ECSSig(b1))hash

[0480] Kt(b2)(+)(UR(b2)||ECSSig(b2))hash。

[0481] 服务器 C 在存储卡的通用区中记录下列数据：内容 Con（c1），与上述内容相对应的使用规则 UR（c1），以及与上述内容相对应的 ECS 文件 ECS（c1）。

[0482] 此外，服务器 C 在存储卡的保护区中的块 #1 中记录下列数据。

[0483] 也就是，记录要应用于内容的解码的标题密钥 Kt（c1）的转换数据的数据，以及

[0484] Kt(c1)(+)(UR(c1)||ECSSig(c1))hash。

[0485] 服务器 D 在存储卡的通用区中记录下列数据：内容 Con（d1）和 Con（d2），与上述内容相对应的使用规则 UR（d1）和 UR（d2），以及与上 述内容相对应的 ECS 文件 ECS（d1）和 ECS（d2）。

[0486] 此外，服务器 D 在存储卡的保护区中的块 #1 中记录下列数据。

[0487] 也就是，记录要应用于内容的解码的标题密钥 Kt（d1）和 Kt（d2）的转换数据的数据，以及

[0488] Kt(d1)(+)(UR(d1)||ECSSig(d1))hash

[0489] Kt(d2)(+)(UR(d2)||ECSSig(d2))hash。

[0490] 当再现内容的用户装置（主机）从通用区选择将再现的内容时，需要指定保护区中的存储有内容的标题密钥的块。

[0491] 从与各个内容相对应的使用规则（UR）中获取用于指定块的信息。

[0492] 参照图 23，将说明使用使用规则的实例。图 23 的（a）示出与记录在存储卡中的通用区中的内容 a1 相对应的使用规则 a1 的具体实例。

[0493] 在使用规则中，记录有下列数据：（1）块标识符（#0）、（2）标题密钥标识符（a1），及（3）ECS 文件标识符（a1）。

[0494] （1）块标识符是指示存储与使用规则 UR（a1）相对应的内容 Con（a1）的标题密钥 Kt（a1）的块的信息。

[0495] 在该实例中，块标识符为 #0，再现内容的用户（主机装置）可以选择块 #0。

[0496] （2）标题密钥标识符是指示哪一个标题密钥是存储在块 #0 上的多个标题密钥中的与使用规则 UR（a1）相对应的内容 Con（a1）的标题密钥的信息。

[0497] 在该实例中，标题密钥标识符＝ a1，可选择标题密钥 Kt（a1）。

[0498] （3）ECS 文件标识符（a1）是用于标识与内容（a1）相对应的 ECS 文件的信息。

[0499] 用户装置（主机）参照使用规则 UR（a1）确认保护区中存储要使用的内容 Con（a1）的标题密钥的块，并且从该块中读取下列数据：

[0500] Kt(a1)(+)(UR(a1)||ECSSig(a1))hash。

[0501] 接着，执行用于耦合从通用区读取的 ECS 文件 ECS（a1）上存储的 ECS 发布方签名（ECSSig xy）和使用规则 UR（a1）的处理，并且执行用于计算哈希值的处理。

[0502] 也就是，计算 P(a1)=(UR(a1)||ECSSig(a1))hash。

[0503] 此后，通过执行下列计算获取标题密钥 Kt（xy）：

[0504] [从块读取的数据(标题密钥转换数据)](+)P(xy)

[0505] =(Kt(a1)(+)(UR(a1)||ECSSig(a1))hash)(+)P(a1)

[0506] =(Kt(a1)(+)(UR(a1)||ECSSig(a1))hash)(+)(UR(a1)||ECSSig(a1))hash)

[0507] =Kt(a1)

[0508] 标题密钥 Kt（a1）是通过计算处理获取的，利用获取的标题密钥解码和使用加密内容。

[0509] 如上所述，记录在存储卡中的保护区中的标题密钥被存储为与使用规则(UR)和 ECS 发布方签名(ECSSig)的耦合数据的哈希值的异或(XOR)计算结果。

[0510] 通过执行这种处理，即使在泄露将被应用到 ECS 发布方签名(ECSSig)的 ECS 发布方的签名密钥(秘密密钥)的情况下，也能防止内容的不当使用。

[0511] 例如，内容提供服务器和用户装置可以防止通过应用 ECS 发布方的泄露签名密钥(秘密密钥)的不当处理(具体为用于替换加密内容的处理)进行的内容的不当使用。

[0512] 此外，“替换”意味着用于使用与特定内容(C1)相对应的标题密钥(Kt1)加密其它内容(C2)、(C3)、(C4)、…，并且将该内容提供给用户的处理。

[0513] 如果执行这种替换处理，在无需合法地购买内容(C2)、(C3)、(C4)、…的情况下拥有标题密钥(Kt1)的用户装置能解码和再现其它内容(C2)、(C3)、(C4)。

[0514] 通过将记录在存储卡的保护区中的标题密钥存储为与使用规则(UR)和 ECS 发布方签名(ECSSig)之间的耦合数据的哈希值的异或(XOR)计算结果，能防止上述替换。

[0515] 将参照图 24 及后续附图说明通过防止替换获取的效果。

[0516] 图 24 的(a)示出用于存储与内容(C1)相对应的得当数据的配置，图 24 的(b)示出用于存储通过利用与内容(C1)相对应的标题密钥(Kt1) 加密内容(C2)的替换数据的配置。

[0517] 在图 24 的(a)示出的用于存储得当数据的配置中，存储卡的通用区中记录有：(a1)利用用于内容(C1)的得当标题密钥(Kt1)加密的加密内容(C1 (Kt1)，(a2)用于内容(C1)的得当使用规则(UR1)，和(a3)用于内容(C1)的得当加密内容签名文件(ECS 文件 ECS1 (C1，Kt1))。

[0518] 另外，ECS 发布方签名(ECSSig)被存储在 ECS 文件上，且 ECS 发布方签名(ECSSig)包括基于包括如上参照图 13 描述的标题密钥(Kt1)的哈希值的数据所生成的内容(C1)的哈希列表集和电子签名。为了清楚显示签名数据的生成源上的数据，将 ECS 文件描述为 ECS1 (C1，Kt1)。

[0519] 另外，在用于存储图 24 的(a)中所示的得当数据的配置中，标题密钥(Kt1)的转换数据(即下列数据)被记录在存储卡的保护区中的块 N 上：Kt1(+)(UR1||ECS1Sig)hash，其中，UR1 表示用于内容 1 的使用规则，ECS1Sig 表示作为与内容 1 相对应的 ECS 文件的配置数据的 ECS 发布方的签名。

[0520] 另外，作为元算符的符号的意义如下。也就是，(+) 表示异或运算，|| 表示数据耦合，a ||b 意味着数据 a 和数据 b 的耦合数据。“hash”表示哈希值，“(a||b)hash”意思是数据 a 和数据 b 的耦合数据的哈希值。

[0521] 例如，恶意内容提供服务器将用于内容(C1)的标题密钥(Kt1)作为用于另一内容(C2)的加密密钥提供给用户。

[0522] 作为传输不当内容的结果，图 24 的(b)中示出的“替换数据”被存储在存储卡上。

[0523] 在图 24 的(b)中所示的用于存储“替换数据”的配置中，在存储卡的通用区上存储有：(b1)利用用于内容(C2)的不当标题密钥(Kt1)加密的不当加密内容(C2 (Kt1))，(b2)与内容(C2)不当关联的使用规则(UR1)(＝对应于内容(C1)的使用规则(UR1))，和(b3)不当生成的与内容(C2)对应的加密内容签名文件(ECS2)(=ECS2 (C2，Kt1))。

[0524] 另外，不当 ECS 文件(即存储在 ECS2 上的 ECS 发布方签名(ECSSig))包括基于 ECS 发布方的泄露的签名密钥(秘密密钥)所生成的电子签名和内容(C2)的哈希列表集，ECS 发布方的泄露的签名密钥(秘密密钥)所基于的数据包括与内容(C1)相对应的标题密钥(Kt1)的哈希值。为了清楚地示出签名数据的生成源的数据，将 ECS 文件示出为 ECS2(C2，Kt1)。

[0525] 另外，在存储图 24 的(b)所示的“替换数据”的配置中，标题密钥(Kt1)的转换数据(即下列数据)被记录在存储卡的保护区中的块 N 上：Kt1(+)(UR1||ECS1Sig)hash。

[0526] 将参照图 25 所示的流程图说明用于记录图 24 的(b)中所示的“替换数据”的处理序列。

[0527] 另外，图 25 中所示的处理是利用存储有与如图 24 的(a)上面所示的内容(C1)对应设置的得当数据的存储卡执行的、以及由拥有作为对存储卡上的保护区中的块 N 的访问权的执行数据读取处理的权利的设备执行的处理，例如该设备是内容提供服务器或用户装置。

[0528] 首先，在步骤 S201 中，制备新内容 C2。

[0529] 接着，在步骤 S202 中，从记录在存储卡的通用区中的用于内容(C1)的使用规则(UR1)获取“块标识符”和“标题密钥标识符”，并且基于获取的信息从预定的块(即在保护区中的存储有标题密钥的块)读取下列与得当内容(C1)对应的标题密钥转换数据：

[0530] Kt1(+)(UR1||ECS1Sig)hash。

[0531] 另外，ECS1Sig=Sign(ECS 签名密钥，M)，M= 内容 C1 的内容哈希列表集 ||Kt1 哈希值。

[0532] 接着，在步骤 S203 中，计算与从通用区读取的内容(C1)相对应的使用规则(UR1)和 ECS 文件(ECS1 (C1，Kt1))之间耦合数据的哈希值，对计算结果与从保护区读取的标题密钥转换数据之间进行异或运算，以获取与内容(C1)相对应的得当标题密钥(Kt1)。

[0533] 也就是，基于下列等式获取标题密钥(Kt1)：

[0534] Kt1=(从保护区读取的数据)(+)(从通用区读取的数据)

[0535] =Kt1(+)(UR1||ECS1Sig)hash(+)(UR1||ECS1Sig)hash。

[0536] 另外，(+) 表示异或(XOR)。

[0537] 接着，在步骤 S204 中，应用在步骤 S203 中获取的标题密钥(Kt1)，执行新内容(C2)的加密。

[0538] 生成加密内容 C2 (Kt1)。

[0539] 接着，在步骤 S205 中，将加密内容 C2 (Kt1)记录在存储卡的通用区中。

[0540] 接着，在步骤 S206 中，生成用于根据内容 C2 生成的 Kt1 哈希值和内容哈希列表集的加密内容签名 ECS2Sig。也就是，生成如下签名数据：ECS2Sig=Sign(ECS 签名密钥，M)，其中，

[0541] M= 内容 C2 的内容哈希列表集 ||Kt1 哈希值。

[0542] 另外，加密内容签名发布方的泄露的签名密钥(秘密密钥)被应用于生成签名。

[0543] 最后，在步骤S207中，生成包括在步骤S206中不当生成的ECS签名(ECS2Sig(C2，Kt1)的ECS文件，并将其记录在存储卡的通用区。

[0544] 通过图25所示的一系列处理，完成图24的(b)所示的用于记录“替换数据”的处理。

[0545] 通过上述替换处理，生成通过利用用于不同内容(C1)的标题密钥(Kt1)加密内容C2获取的内容C2（Kt1)。

[0546] 在该实例中，假定内容C1的使用规则(UR1)被原样使用，作为与不当记录内容C2(Kt1)相对应的使用规则。

[0547] 接着，将参照图26所示的流程图说明用户装置利用图24的(b)所示的“替换数据”再现内容C2时的处理。

[0548] 首先，在步骤S221中，用户装置从存储卡的通用区读取将再现的加密内容C2(Kt1)和为该内容生成的ECS文件(ECS2（C2，Kt1))。

[0549] 接着，在步骤S222中，用户装置从存储卡的通用区从记录成与内容C2对应的使用规则(UR1)中读取表示存储有标题密钥的块的块标识符。

[0550] 如上所述，在该实例中，用于内容C1的使用规则(UR1)被原样使用，作为与不当记录内容C2（Kt1)相对应的使用规则。

[0551] 如上面参照图23所述，使用规则(UR)中记录有存储有标题密钥的块标识符、标题密钥标识符等。

[0552] 在步骤S222中，用户装置从用于内容C1的使用规则(UR1)中读取块标识符和标题密钥标识符。

[0553] 块标识符是与存储与内容C1相对应的得当标题密钥Kt1的块相对应的标识符，标题密钥标识符是与存储在块上的标题密钥相对应的标识符。

[0554] 因此，读取用于内容C1的标题密钥转换数据，即：

[0555] Kt1(+)(UR1||ECS1Sig)hash)。

[0556] 接着，在步骤S223中，用户装置计算从通用区读取的使用规则(UR1)和不当生成为与内容C2对应的ECS文件(ECS2（C2,Kt1))之间的耦合数据的哈希值，并且执行计算结果与从保护区读取的标题密钥转换数据之间的异或(XOR)，以试图获取用于对应于内容C2进行解码的标题密钥Kt2。

[0557] 这里，如果能获取满足Kt2=Kt1的标题密钥Kt2，则成功获取标题密钥。

[0558] 也就是，用户装置试图基于下列等式执行用于计算标题密钥的处理：Kt2=(从保护区读取的数据)(+)(从通用区读取的数据)

[0559] =Kt1(+)(UR1||ECS2Sig)hash(+)(UR1||ECS1Sig)hash。

[0560] 用户装置试图基于用于计算标题密钥的上述等式获取标题密钥(Kt2)。

[0561] 另外，(+)意思是异或(XOR)。

[0562] 然而，由于在用于计算标题密钥的上述等式中ECS2Sig ≠ ECS1Sig，通过上述等式获取的值Kt2是与Kt1不同的值，也就是得到关系式Kt2 ≠ Kt1。

[0563] 结果，不获取应用于内容C2的加密的标题密钥Kt1，且用户装置不能解码和再现内容C2。这与步骤S224中的处理对应。

[0564] 在步骤 S225 中，用户装置基于预定的再现序列执行用于验证包括在从通用区读取的 ECS 文件中的 ECS 发布方签名（ECSSig）的处理。

[0565] 基于下列式子执行用于验证签名的处理 ：

[0566] Verify （ECE 发布方公共密钥，ECS2Sig，M），

[0567] 其中 Verify(k,S,M)表示用于利用验证密钥 k 验证数据 M 的电子签名 S 的处理。

[0568] M= 内容 C2 的内容哈希列表集 ||Kt2 哈希值。

[0569] 步骤 S223 中计算出的值被用作为 Kt2。

[0570] 存储在 ECS 文件上的 ECS2Sig 是如图 25 所示的流程中的步骤 S206 中生成的不当签名，且为下列数据 ：

[0571] ECS2Sig=Sign(ECS 签名密钥 ,M)，

[0572] 其中，M= 内容 C2 的内容哈希列表集 ||Kt1 哈希值。

[0573] 如上所述，虽然应用到签名验证的数据 M 是包括 Kt2 哈希值的数据，但是为包括 Kt1 哈希值的 M 生成存储在 ECS 文件上的签名数据 ECS2Sig。

[0574] 因此，步骤 S225 中的签名验证失败。这是如图 26 所示的步骤 S226 所说明的。

[0575] 即使用户装置试图通过应用图 24 的（b）所示的“替换数据”来解码和再现内容 C2，用户装置也不能解码内容 C2 并且不能验证 ECS 文件的签名，结果，内容 C2 对于用户装置不可用。

[0576] 如上参照图 24 至图 26 所述的处理实例是用户通过应用用于内容 C1 的标题密钥 Kt1 来加密和解码新内容 C2 的处理实例。

[0577] 接着，将说明与内容 C1 对应的正确的使用规则（UR1）被不当伪造用于生成新的使用规则（UR2）的不当处理的实例。

[0578] 在使用规则中，记载有内容截止日期、复制限制信息等信息，存在通过替换使用规则延长可用时间段的不当行为的可能性。

[0579] 与图 24 的（a）和图 24 的（b）所示的方式相同，图 27 的（a）示出用于存储与内容（C1）相对应的得当数据的配置，图 27 的（b）示出用于存储通过利用与内容（C1）相对应的标题密钥（Kt1）加密内容（C2）的替换数据的配置。

[0580] 在图 27A 中示出的用于存储得当数据的配置中，存储卡的通用区中记录有 ：（a1）利用用于内容（C1）的得当标题密钥（Kt1）加密的加密内容（C1（Kt1），（a2）用于内容（C1）的得当使用规则（UR1），和（a3）用于内容（C1）的得当加密内容签名文件（ECS 文件 ECS1 （C1，Kt1））。

[0581] 另外，ECS 发布方签名（ECSSig）被存储在 ECS 文件上，ECS 发布方签名（ECSSig）包括基于包括如上参照图 13 描述的标题密钥（Kt1）的哈希值的数据生成的电子签名和内容（C1）的哈希列表集。为了清楚地示出签名数据的生成源的数据，将 ECS 文件描述为 ECS1（C1，Kt1）。

[0582] 另外，在用于存储图 27A 所示的得当数据的配置中，标题密钥（Kt1）的转换数据，即下列数据被记录在存储卡的保护区中的块 N 上 ：

[0583] Kt1(+)(UR1||ECS1Sig)hash，

[0584] 其中，UR1 表示用于内容 1 的使用规则，ECS1Sig 表示作为与内容 1 相对应的 ECS 文件的配置数据的 ECS 发布方的签名。

[0585] 另外，作为运算符的符号的意义如下。也就是，(+) 表示异或运算，|| 表示数据耦合，a ||b 意味着数据 a 和数据 b 的耦合数据。“hash”意思是哈希值，“(a ||b)hash”意思是数据 a 和数据 b 的耦合数据的哈希值。

[0586] 例如，恶意内容提供服务器或用户装置重写内容(C1)的使用规则(UR1)。

[0587] 作为不当处理的结果，图 27 的(b)示出的“替换数据”被存储在存储卡上。

[0588] 在图 27B 所示的用于存储“替换数据”的配置中，在存储卡的通用区上存储有：(b1)利用用于内容(C1)的不当标题密钥(Kt2)加密的不当加密内容(C1 (Kt2);(b2)不当生成的与内容(C1)对应的使用规则(UR2);和(b3)不当生成的与内容(C1)对应的加密内容签名文件(ECS2)(=ECS2 (C1,Kt2))。

[0589] 另外，不当 ECS 文件(即存储在 ECS2 上的 ECS 发布方签名(ECSSig))包括基于 ECS 发布方的泄露的签名密钥(秘密密钥)所生成的电子签名和内容(C1)的哈希列表集，ECS 发布方的泄露的签名密钥(秘密密钥)基于包括不当生成标题密钥(Kt2)的哈希值的数据。为了清楚地示出签名数据的生成源的数据，将 ECS 文件描述为 ECS2 (C1,Kt2)。

[0590] 另外，在存储图 27 的(b)中所示的“替换数据”的配置中，标题密钥(Kt1)的转换数据，即下列数据被记录在存储卡的保护区中的块 N 中：Kt1(+)(UR1||ECS1Sig)hash。

[0591] 将参照图 28 所示的流程图说明用于记录图 27 的(b)所示的“替换数据”的处理序列。

[0592] 另外，图 28 中所示的处理是利用存储有如上图 27 的(a)所示的与内容(C1)对应设置的得当数据的存储卡执行的、和由拥有作为对存储卡中的保护区中的块 N 的访问权的执行用于数据读取处理的权利的设备执行的处理，例如该设备是内容提供服务器或用户装置。

[0593] 首先，在步骤 S241 中，从通用区读取与内容 C1 相对应的使用规则 UR1，对可用时段的信息进行如重写等伪造，并生成不当使用规则(UR2)。

[0594] 接着，在步骤 S242 中，从记录在存储卡的通用区中的用于内容(C1)的使用规则(UR1)获取“块标识符”和“标题密钥标识符”，并且基于获取的信息从预定的块(即在保护区中的存储有标题密钥的块)读取下列与得当内容(C1)对应的标题密钥转换数据：

[0595] Kt1(+)(UR1||ECS1Sig)hash，

[0596] 其中，ECS1Sig=Sign(ECS 签名密钥，M)，

[0597] M= 内容 C1 的内容哈希列表集 ||Kt1 哈希值。

[0598] 接着，在步骤 S243 中，计算从通用区读取与得当内容(C1)相对应的使用规则(UR1)和 ECS 文件(ECS1 (C1,Kt1))之间耦合数据的哈希值，并且执行计算结果与从保护区读取的标题密钥转换数据之间的异或，以获取与内容(C1)对应的得当标题密钥(Kt1)。

[0599] 也就是，基于下列等式获取标题密钥(Kt1)：

[0600] Kt1=(从通用区读取的数据)(+)(从保护区读取的数据)

[0601] =(UR1||ECS1Sig)hash(+)Kt1(+)(UR1||ECS1Sig)hash。

[0602] 另外，(+) 表示异或运算(XOR)。

[0603] 此外，基于下列等式计算将应用于加密和解码内容 C2 的标题密钥 Kt2：

[0604] Kt2=(Kt1(+)(UR1||ECS1Sig)hash(+)(UR2||ECS1Sig)hash。

[0605] 接着，在步骤 S244 中，通过应用在步骤 S243 中生成的标题密钥 Kt1 解码内容 C1

(Kt1),还通过应用在步骤 S243 中生成的新的标题密钥 Kt2 加密内容 C1,以获取加密内容 C1 (Kt2)。

[0606] 接着,在步骤 S245 中,将加密内容 C1 (Kt1) 记录在存储卡的通用区中。

[0607] 接着,在步骤 S246 中,生成根据内容 C1 生成的 Kt2 哈希值和内容哈希列表集的加密内容签名 ECS2Sig。也就是,生成如下签名数据 :ECS2Sig=Sign(ECS 签名密钥,M),

[0608] 其中,M= 内容 C1 的内容哈希列表集 ||Kt2 哈希值。

[0609] 另外,加密内容签名发布方的泄露的签名密钥(秘密密钥)被应用于生成签名。

[0610] 接着,在步骤 S247 中,生成包括在步骤 S246 中不当生成的 ECS 签 名(ECS2Sig(C1,Kt1)的 ECS 文件,并将其记录在存储卡的通用区。

[0611] 最后,在步骤 S248 中,将在步骤 S241 中生成的使用规则 UR2 记录在通用区中。

[0612] 通过图 28 所示的一系列的处理,完成图 27 的(b)所示的用于记录“替换数据”的处理。

[0613] 通过上述替换处理,不当生成的使用规则(UR2)与内容 C1 关联。此外,内容 C1 利用新标题密钥 Kt2 加密然后被记录。

[0614] 接着,将参照图 29 所示的流程图说明用户装置利用图 27 的(b)所示的“替换数据”再现内容 C1 时的处理。

[0615] 首先,在步骤 S261 中,用户装置从存储卡的通用区读取要再现的加密内容 C1 (Kt2)和为该内容生成的 ECS 文件(ECS2 (C1,Kt2))。

[0616] 接着,在步骤 S262 中,用户装置从存储卡的通用区从被不当生成为与内容 C1 对应的使用规则(UR2)中读取表示上面存储有标题密钥的块的块标识符和标题密钥标识符。

[0617] 块标识符和标题密钥标识符仍设置为用于伪造前的得当使用规则(UR1)。

[0618] 也就是,块标识符是与存储有用于内容 C1 的得当标题密钥 Kt1 的块的标识符,标题密钥标识符是与存储在块上的标题密钥对应的标识符

[0619] 因此,读取用于内容 C1 的标题密钥转换数据(即 Kt1(+)(UR1||ECS1Sig)hash)。

[0620] 接着,在步骤 S263 中,计算从通用区读取的不当生成的使用规则(UR2)和不当生成的 ECS 文件(ECS2 (C1,Kt2))之间的耦合数据的哈希值,并且对计算结果与从保护区读取的标题密钥转换数据之间进行异或(XOR)运算,以试图获取用于解码与内容 C1 对应的标题密钥 Kt3。

[0621] 这里,如果能获取满足 Kt3=Kt2 的标题密钥 Kt2,则成功获取标题密钥。

[0622] 也就是,用户装置试图基于下列等式执行用于计算标题密钥的处理 :Kt3=(从保护区读取的数据)(+)(从通用区读取的数据)

[0623] =Kt1(+)(UR1||ECS1Sig)hash(+)(UR2||ECS2Sig)hash。

[0624] 基于用于计算标题密钥的上述等式生成标题密钥(Kt3)。

[0625] 此外,(+) 意思是异或运算(XOR)。

[0626] 然而,不能通过用于计算标题密钥的上述等式获取 Kt2。

[0627] 通过上述等式获取的值 Kt3 是与 Kt1 和 Kt2 不同的值,也就是得到关系式 $Kt3 \neq Kt2$ 和 $Kt3 \neq Kt1$。

[0628] 结果,不能获取适用于重新加密内容 C1 的标题密钥 Kt2,用户装置不能解码和再现内容 C1。这与步骤 S264 中的处理对应。

[0629] 在步骤 S265 中，用户装置基于预定的再现序列执行用于验证包括在从通用区读取的 ECS 文件中的 ECS 发布方签名（ECSSig）的处理。

[0630] 也就是，用户装置基于下列式子执行用于签名验证处理 ：

[0631] Verify （ECE 发布方公共密钥，ECS2Sig，M），

[0632] 其中 Verify （k，S，M）表示利用验证密钥 k 用于验证用于数据 M 的电子签名 S 的处理。M= 内容 C1 的内容哈希列表集 ||Kt3 哈希值。

[0633] 使用在步骤 S263 中计算出的值作为 Kt3。

[0634] 存储在 ECS 文件中的 ECS2Sig 是如图 28 所示的流程中的步骤 S246 中生成的不当签名，且为下列数据 ：

[0635] ECS2Sig=Sign(ECS 签名密钥，M)，

[0636] 其中，M= 内容 C1 的内容哈希列表集 ||Kt2 哈希值。

[0637] 如上所述，虽然应用到签名验证的数据 M 是包含 Kt3 哈希值的数据，但是存储在 ECS 文件上的签名数据 ECS2Sig 是生成为用于包含 Kt2 哈希值的 M。

[0638] 因此，步骤 S265 中的签名验证失败。这是图 29 所示的步骤 S266 所说明的。

[0639] 即使用户装置试图通过应用图 27B 所示的“替换数据”来解码和再现内容 C1，用户装置也不能解码内容 C1 并且不能验证 ECS 文件的签名，结果内容 C1 对于用户装置不可用。

[0640] 通过将存储在存储卡中的保护区中的标题密钥作为使用规则（UR）和 ECS 发布方签名（ECSSig）之间的耦合数据的哈希值的异或运算（XOR）结果存储，即使在泄露将应用到 ECS 发布方签名（ECSSig）的 ECS 发布方的签名密钥（秘密密钥）的情况下，也能防止内容的不当使用。

[0641] 例如，内容提供服务器和用户装置可通过对应用 ECS 发布方的泄露的签名密钥（秘密密钥）的不当处理来防止内容的不当使用，具体为用于替换加密内容的加密密钥的处理、使用规则的伪造等。

[0642] [11、关于用于应用记录在加密内容签名（ECS）文件中块标识符的处理]

[0643] 接着，将说明用于应用记录在加密内容签名（ECS）文件中块标识符（PAD 块编号）的处理。

[0644] 如上参照图 9A 和图 9B 所述，块标识符（PAD 块编号）被记录在加密内容签名（ECS）文件中。

[0645] 块标识符（PAD 块编号）是如上参照图 13 所述的从内容提供方（内容服务器）103 传输到加密内容签名（ECS）发布方 102 的数据，块标识符（PAD 块编号）是介质中的保护区中的上面存储有作为与内容提供方 103 提供给用户装置 104 的内容对应加密密钥的标题密钥的块的标识符。其是介质中的保护区中的内容提供方 103 可使用的块的标识符。

[0646] 如参照图 3 和图 6 等所述，介质中的保护区中的内容提供方可使用的块被预先设置，并且记录有访问允许块信息。

[0647] 此外，与块标识符（PAD 块编号）对应的信息还记录在如上参照图 9A 和图 9B 所述的 ECS 发布方证书中。

[0648] 如上参照图 9A 和图 9B 所述，记录有（a）块标识符开始编号（开始 PAD 块编号）和（b）块标识符范围（PAD 块编号计数器）。

[0649] (a)块标识符开始编号(开始PAD块编号)是介质中的保护区中的ECS发布方102可允许内容提供方103访问的访问允许块的起始编号。

[0650] (b)块标识符范围(PAD块编号计数器)是表示从介质中的保护区中的ECS发布方102可允许内容提供方103访问的访问允许块的起始编号起算的范围的信息。

[0651] 此外,块标识符还记录在与如上参照图23所述的内容对应的使用规则(UR)中。记录在使用规则(UR)中的块标识符是指示存储有与内容对应的标题密钥的块的块标识符。

[0652] 图30示出加密内容签名(ECS)文件、使用规则和保护区中的记录在其中的块标识符和标题密钥存储块(在图中的实例中示出为块k)之间的对应关系。

[0653] 如图30所示,存储块的通用区存储有加密内容签名(ECS)文件和与内容对应的使用规则(UR)的数据。

[0654] 此外,保护区的块k中存储有与内容对应的标题密钥转换数据,即Kt(+)UR||ECSSig)hash。

[0655] 将内容提供给用户这种的内容提供方将作为记录在其主机证书(见图5)中的保护区访问权的信息的块标识符与作为ECS发布方证书中的块标识符的写入允许块区的信息进行比较。

[0656] 内容提供方根据比较结果确定是否能提供内容。

[0657] 此外,再现内容的用户装置将使用规则中的块标识符与ECS文件中的块标识符进行比较。

[0658] 用户装置根据比较结果确定是否能再现内容。

[0659] 首先,将参照图31所示的流程图说明用于利用内容提供服务器的块标识符来确定是否能提供内容的序列。

[0660] 此外,作为图31所示的流程图的步骤S401的预处理,内容提供方通过应用设置在从加密内容签名文件(ECS文件)发布方接收的加密内容签名文件(ECS文件)来执行签名验证。

[0661] 当成功进行签名验证并且确认加密内容签名文件(ECS文件)有效时,内容提供方还对存储在加密内容签名文件(ECS文件)上的ECS发布方证书执行签名验证。在两种签名验证成功完成的条件下,执行步骤S401及后续步骤中的处理。

[0662] 当上述两种签名验证中的至少一个未成功进行时,未确认加密内容签名文件(ECS文件)的有效性或ECS发布方证书的有效性,因此,不执行步骤S401及后续步骤中的处理。在该情况下,也不执行提供内容的处理。

[0663] 关于作为存储在加密内容签名文件(ECS文件)上的内容哈希列表集的初始源的内容哈希,可设置为加密前的内容哈希和加密后的内容哈希中的任意一个。

[0664] 当对加密内容签名文件(ECS文件)和的ECS发布方证书的两种签名验证成功完成时,确认加密内容签名文件(ECS文件)的有效性和ECS发布方证书的有效性,内容提供方执行步骤S401中的处理。

[0665] 首先,在步骤S401中,内容提供方读取ECS文件中的ECS发布方 证书,并且读取记录在ECS发布方证书中的块标识符信息。

[0666] 将参照图32所示的流程详细说明步骤S401中的处理。

[0667] 在步骤S421中,读取ECS发布方证书中的块标识符开始编号(开始PAD块编号)。

[0668] 块标识符开始编号(开始PAD块编号)是是介质中的保护区中的ECS发布方102可允许内容提供方103访问的访问允许块的起始编号。

[0669] 接着,在步骤S422中,确定ECS发布方证书中的块标识符开始编号(开始PAD块编号)是否是0×FFFFFFFF。

[0670] 块标识符开始编号(开始PAD块编号)是0×FFFFFFFF的情况与允许访问所有块的情况对应。

[0671] 当在步骤S422中确定块标识符开始编号(开始PAD块编号)是0×FFFFFFFF时,处理执行到步骤S423,在介质中的保护区中设置的在前块被视为访问允许块。

[0672] 另一方面,在步骤S422中确定块标识符开始编号(开始PAD块编号)不是0×FFFFFFFF时,处理执行到步骤S424。

[0673] 在步骤S424中,读取ECS发布方证书中的块标识符范围信息(PAD块编号计数器)。

[0674] 块标识符范围(PAD块编号计数器)是表示从介质中的保护区中的ECS发布方102可允许内容提供方103访问的访问允许块的起始编号起算的范围的信息。

[0675] 步骤S425至S428中接着处理的步骤是重复执行的程序,其中,表示块标识符的变量I顺次从0递增到1、2、3…。

[0676] 首先,在步骤S425中,变量I被设置为满足I=1。

[0677] 接着,在步骤S426中,块标识符开始编号(开始PAD块编号)+I被增加到块标识符表(PAD块编号表)。

[0678] 接着,在步骤S427中,I被设置为满足I=I+1。

[0679] 接着,在步骤S427中,确定I是否等于块标识符范围信息(PAD块编号计数器)。

[0680] 当I等于块标识符范围信息(PAD块编号计数器)时,完成处理。当I不等于块标识符范围信息(PAD块编号计数器)时,处理返回到步骤 S426并且重复程序。

[0681] 基于上述处理,执行图31所示的流程图中所示的步骤S401中的处理。

[0682] 在步骤S401中,ECS发布方证书中的块标识符开始编号(开始PAD块编号)和块标识符范围信息(PAD块编号计数器)被应用于计算ECS发布方证书中的预定的访问允许范围,访问允许范围被设置作为访问允许块标识符表。

[0683] 接着,在步骤S402中,确定记录在加密内容签名(ECS)文件中的数据描述的块标识符开始编号(开始PAD块编号)是否包括在步骤S401中生成的访问允许块标识符表中。

[0684] 当块标识符开始编号(开始PAD块编号)未被包括在访问允许块标识符表中时,处理执行到步骤S405,并且不执行将内容提供给用户装置的处理。

[0685] 另一方面,当块标识符开始编号(开始PAD块编号)被包括在访问允许块标识符表中时,处理执行到步骤S403。

[0686] 在步骤S403中,确定记录在加密内容签名(ECS)文件中的数据所述的块标识符开始编号(开始PAD块编号)是否与使用规则(UR)中所述的块标识符一致。

[0687] 当块标识符开始编号(开始PAD块编号)与使用规则(UR)中所述的块标识符不一致时,处理执行到步骤S405,并且不执行用于将内容提供给用户装置的处理。

[0688] 另一方面,当块标识符开始编号(开始PAD块编号)与使用规则(UR)中所述的块标识符一致时,处理执行到步骤S404,并且执行用于将内容提供给用户装置的处理。

[0689] 如上所述,内容提供方确定是否满足条件(a)记录在加密内容签名(ECS)文件中

的块标识符开始编号(开始PAD块编号)位于记录在ECS发布方证书中的访问允许块范围中和(b)记录在加密内容签名(ECS)文件中的块标识符开始编号(开始PAD块编号)与使用规则(UR)中记录的块标识符一致,只有当条件满足时,内容提供方才将内容提供给用户装置。

[0690] 接着,将参照图33所示的流程图说明执行用于再现内容的处理的用户装置应用块标识符的处理。

[0691] 在图33所示的步骤S451之前,用户装置通过应用设置在从内容提供方接收的加密内容签名文件(ECS文件)来执行签名验证。

[0692] 当成功进行签名验证并且确认加密内容签名文件(ECS文件)有效时,用户装置还对存储在加密内容签名文件(ECS文件)上的ECS发布方证书执行签名验证。在两种签名验证成功完成的条件下,执行步骤S451及后续步骤中的处理。

[0693] 当上述两种签名验证中的至少一个未成功进行时,未确认加密内容签名文件(ECS文件)的有效性或ECS发布方证书的有效性,因此,不执行步骤S451及后续步骤中的处理。在该情况下,也不执行再现内容的处理。

[0694] 当对加密内容签名文件(ECS文件)和的ECS发布方证书的两种签名验证成功完成时,确认加密内容签名文件(ECS文件)的有效性和ECS发布方证书的有效性,用户装置执行步骤S451中的处理。

[0695] 在步骤S451中,处理与作为内容提供方的处理的如上参照图31所述的流程中的步骤S401中的处理相同。也就是,如具体参照图32所述的流程,ECS发布方证书中的块标识符开始编号(开始PAD块编号)和块标识符范围信息(PAD块编号计数器)被应用于计算ECS发布方证书中的预定的访问允许范围,访问允许范围被设置作为访问允许块标识符表。

[0696] 接着,在步骤S452中,确定记录在加密内容签名(ECS)文件中的数据所述的块标识符(PAD块编号)是否被包含在步骤S451中生成的访问允许块标识符表中。

[0697] 当确定块标识符(PAD块编号)未被包含在访问允许块标识符表中时,处理执行到步骤S455,并且不执行再现内容的处理。

[0698] 另一方面,当确定块标识符开始编号(开始PAD块编号)被包含在访问允许块标识符表中时,处理执行到步骤S453。

[0699] 在步骤S453中,确定记录在加密内容签名(ECS)文件中的数据所述的块标识符(PAD块编号)是否与使用规则(UR)中记录的块标识符一致。

[0700] 当块标识符(PAD块编号)与使用规则(UR)中记录的块标识符不一致时,处理执行到步骤S455,并且不执行再现内容的处理。

[0701] 另一方面,当块标识符(PAD块编号)与记录在使用规则(UR)中 的块标识符一致时,处理执行到步骤S454,并且执行用于再现内容的处理。

[0702] 在开始用于再现内容的处理之前,执行用于获取和生成将应用于加密内容的解码的标题密钥的处理,以及通过应用包括在加密内容签名文件中的内容哈希列表来进行交叉校验哈希值的处理。当在哈希值的交叉校验中成功进行交叉校验时,确认内容未进行伪造,允许内容的再现。

[0703] 如上所述,再现内容的用户装置确定是否满足条件(a)记录在加密内容签名(ECS)文件中的块标识符(PAD块编号)位于记录在ECS发布方证书中的访问允许块范围中和(b)记录在加密内容签名(ECS)文件中的块标识符(PAD块编号)与使用规则(UR)中记录

的块标识符一致，只有当条件满足时，内容装置才再现内容。

[0704] [12、关于各个设备的硬件配置实例]

[0705] 最后，将参照图 34 说明执行上述处理的各个设备的硬件配置实例。

[0706] 图 34 示出可适用于图 7 和图 8 所示的用户装置 104、内容提供方 103 加密内容签名发布方 102 和许可发布方 101 中的任意一个的信息处理设备的硬件配置实例。

[0707] CPU（中央处理单元）701 用作基于存储在 ROM（只读存储器）702 或存储单元 708 上的程序执行各种处理的数据处理单元。例如，CPU701 基于上述各个流程图执行处理。RAM（随机访问存储器）703 在其上适当地存储将被 CPU701 执行的程序、数据等。CPU701、ROM702 和 RAM703 经由总线 704 彼此连接。

[0708] CPU701 经由总线 704 连接到输入输出接口 705，输入单元 706 和输出单元 707 连接到输入输出接口 705，输入单元 706 包括各种开关、键盘、鼠标、麦克风等，输出单元 707 包括显示器、扬声器等。例如，CPU701 响应从输入单元 706 输入的指令执行各种处理并且将处理结果输出到输出单元 707。

[0709] 连接到输入输出接口 705 的存储单元 708 是由硬盘等配置成，并且存储有 CPU701 将执行的程序和各种数据。通信单元 709 经由诸如互联网或局域网与外部装置通信。

[0710] 连接到输入输出接口 705 的驱动器 710 驱动诸如磁盘、光盘、磁光盘等可移动介质 711，或诸如存储卡等半导体存储器，并且获取诸如记录内容等各种数据和密钥信息。例如，基于 CPU 执行的再现程序利用获取的 内容或密钥数据进行解码和再现内容的处理。

[0711] 图 35 示出作为信息存储设备的存储卡的硬件配置实例。

[0712] CPU（中央处理单元）801 用作基于存储在 ROM（只读存储器）802 或存储单元 807 上的程序执行各种处理的数据处理单元。例如，CPU801 执行如上面实施例中所述的处理：用于服务器或主机装置通信；用于从存储单元 807 读取数据或向其写入数据；用于确定是否能允许访问存储单元 807 中的保护区 811 中的分区单元等。RAM（随机访问存储器）803 在其上适当地存储 CPU801 所执行的程序、数据等。CPU801、ROM802 和 RAM803 经由总线 804 彼此连接。

[0713] CPU801 经由总线 804 连接到输入输出接口 805，通信单元 806 和存储单元 807 连接到输入输出接口 805。

[0714] 连接到输入输出接口 805 的通信单元 806 例如与服务器或主机通信。存储卡单元 807 是数据存储区，并且包括如上所述的访问受限的保护区 811 和能自由读写数据的通用区 812。

[0715] 尽管在上述实施例中以内容提供方所提供的内容为加密内容为代表实例进行了上述说明，但是本发明的配置不限于提供的内容是加密内容的情况，还可适用于未加密纯文本内容。在纯文本内容的情况下，可执行与上述用于提供加密内容的处理相同的处理，但是已知的数据序列（例如密钥数据的全部值为零）被用作上述实施例中的标题密钥。

[0716] [13、根据本发明的配置的结论]

[0717] 上面参照具体实施例对本发明的实施例进行了具体说明。然而，对本领域的普通技术人员显而易见的是，在不背离本发明的范围的前提下，可对实施例进行修改和替换。也就是，本发明这里的说明仅为示例性的目的而不做排它性理解。为了确定本发明的保护范围，应考虑随附的权利要求书。

[0718] 另外，这里公开的技术可实施为下列配置。

[0719] （1）一种信息处理设备包括：数据处理单元，执行用于解码和再现加密内容的处理，其中，数据处理单元通过应用与要再现的内容相对应设置的加密内容签名文件来执行用于确定内容是否能被再现的处理，其中，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，其中，在用于确定内容是否 能被再现的处理中，数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期信息进行比较，当加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，不执行用于解码和再现加密内容的处理，以及仅当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，执行用于解码和再现加密内容的处理。

[0720] （2）根据（1）所述的信息处理设备，其中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元还：参考撤销列表，撤销列表记录有加密内容签名发布方证书的失效的信息，以及在确认加密内容签名发布方证书的标识符未被登记在撤销列表中的条件下，执行用于解码和再现加密内容的处理。

[0721] （3）根据（1）或（2）所述的信息处理设备，其中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元还：参考撤销列表，撤销列表记录有加密内容签名发布方证书的失效的信息，以及当加密内容签名发布方证书的标识符被登记在撤销列表中时，从撤销列表获取加密内容签名发布方证书的失效日期，并且在确认加密内容签名文件的发布日期在失效日期之前的条件下，执行用于解码和再现加密内容的处理。

[0722] （4）根据（1）-（3）中的任一项所述的信息处理设备，其中，加密内容签名文件是这样的文件，其包括：内容的哈希值；以及用于包括应用于内容的解码的密钥信息和加密内容签名文件的发布日期的信息的数据的电子签名；以及在通过对电子签名执行签名验证确认加密内容签名文件未作假之后，数据处理单元执行用于确定内容是否能被再现的处理。

[0723] （5）根据（1）-（4）中的任一项所述的信息处理设备，其中，加密内容签名发布方证书中设置有许可发布方的电子签名，在通过对电子签名执行签名验证确认加密内容签名发布方证书未作假之后，数据处理单元执行用于确定内容是否能被再现的处理。

[0724] （6）一种信息处理设备包括：一种信息处理设备，包括：数据处理单元，执行用于向用户装置提供加密内容的处理，其中，数据处理单元通过应用与加密内容对应设置的加密内容签名文件来执行用于确定内容是否能被提供的处理，其中，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书， 其中，在用于确定内容是否能被提供的处理中，数据处理单元：将记录在加密内容签名发布方证书中的加密内容签名发布方证书的截止日期与加密内容签名文件的发布日期的信息进行比较，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，参考记录有加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理，以及当确认加密内容签名发布方证书的截止日期在加密内容签名文件的发布日期之前时，参考加密内容签名发布方证书的截止日期的信息，执行用于确定内容

是否能被提供的处理。

[0725] （7）根据（6）所述的信息处理设备，其中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元将加密内容签名发布方证书的截止日期与实际时间进行比较，如果加密内容签名发布方证书的截止日期在实际时间之前，则数据处理单元不执行用于向用户装置提供加密内容的处理。

[0726] （8）根据（6）或（7）所述的信息处理设备，其中，当确认加密内容签名发布方证书的截止日期不在加密内容签名文件的发布日期之前时，数据处理单元将加密内容签名发布方证书的截止日期与实际时间进行比较，当加密内容签名发布方证书的截止日期不在实际时间之前时，将加密内容签名文件的发布日期与实际时间进行比较，当加密内容签名文件的发布日期在实际时间之前时，不执行用于向用户装置提供加密内容的处理。

[0727] （9）根据（8）所述的信息处理设备，其中，当确认加密内容签名文件的发布日期不在实际时间之前时，数据处理单元进一步参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表，执行用于确定内容是否能被提供的处理。

[0728] （10）根据（6）-（9）中的任一项所述的信息处理设备，其中，数据处理单元参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表，并且在确认加密内容签名发布方证书的标识符未被登记在撤销列表中的条件下，执行用于向用户装置提供加密内容的处理。

[0729] （11）根据（6）-（10）中的任一项所述的信息处理设备，其中，数据处理单元参考其中记录有加密内容签名发布方证书的失效的信息的撤销列表来执行用于确定内容是否能被提供的处理，当加密内容签名发布方证书的标识符被登记在撤销列表中时，从撤销列表获取加密内容签名发布方证书的失效日期，并且在确认加密内容签名文件的发布日期在失效日期之前的条件下，执行用于向用户装置提供加密内容的处理。

[0730] （12）一种信息处理系统包括：一种信息处理系统，包括：用户装置，其执行用于再现内容的处理；内容提供方，其执行用于将内容提供给用户装置的处理；以及加密内容签名发布方，其执行用于将加密内容签名文件提供给内容提供方的处理，其中，内容提供方将内容哈希列表集和内容加密密钥或加密密钥的哈希值发送到加密内容签名发布方，内容哈希列表集包括以内容的配置数据为基础的哈希值，加密内容签名发布方：生成用于作为签名目标的数据的签名数据，作为签名目标的数据是包括内容哈希列表集、内容加密密钥的哈希值和生成加密内容签名文件的日期的信息的数据；生成包括所生成的签名数据和内容哈希列表集的加密内容签名文件；以及将加密内容签名文件发送给内容提供方，内容提供方通过应用生成加密内容签名文件的日期的信息来执行用于确定内容是否能被提供的处理，以及用户装置通过应用生成加密内容签名文件的日期的信息来执行用于确定内容是否能被再现的处理。

[0731] （13）一种信息存储设备包括：一种信息存储设备，包括：存储单元，其存储加密内容和将用于加密内容的解码的加密密钥，其中，存储单元包括保护区和通用区，保护区上存储有作为加密密钥的转换数据的转换加密密钥，保护区设置有访问限制，并且通用区上存储有加密内容，通用区上存储有与加密内容对应设置的加密内容签名文件，加密内容签名文件是这样的文件，其上存储有：加密内容签名文件的发布日期的信息，以及具有作为生成加密内容签名文件的设备的加密内容签名发布方的公共密钥的加密内容签名发布方证书，

使执行用于从存储单元读取并且再现加密内容的处理的再现设备通过应用加密内容签名文件的发布日期的信息来确定内容是否能被再现。

[0732] (14)根据(13)所述的信息存储设备，其中，加密内容签名文件包括用于发布日期的信息的电子签名，以及使执行用于从存储单元读取并且再现加密内容的处理的再现设备对加密内容签名文件的电子签名执行验证处理，并且在成功进行验证的条件下，通过应用发布日期的信息来确定内容是否能被再现。

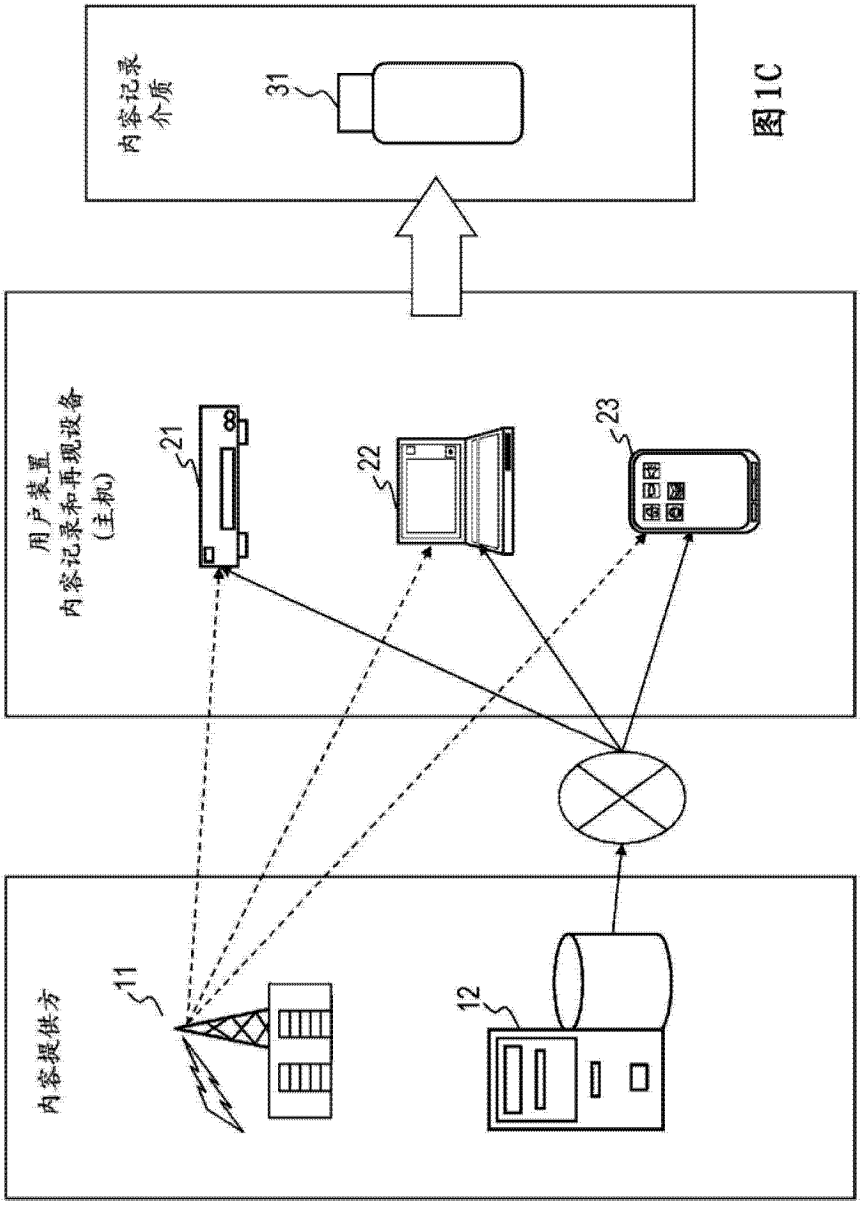
[0733] 此外，在本发明的配置中还包括在上述设备和系统中实施的用于使上述设备和系统执行处理的处理方法和程序。

[0734] 另外，这里所述的系列程序可通过硬件、软件或两者组合配置来执行。当通过软件来执行处理时，其中记录有处理序列的程序被安装在埋设在专用硬件的计算机中的存储器中且在存储器中执行，或者可将程序安装在可 执行各种处理的通用计算机中且在通用计算机中执行程序。例如，程序可预先记录在记录介质中。程序不仅可从记录介质安装到计算机，而且可经由如 LAN (局域网)或互联网等网络接收并且被安装在如埋设式硬盘等记录介质中。

[0735] 另外，根据执行处理的设备的处理能力，这里所述的各种处理可根据需要以所述顺序按照时间顺次的方式执行，或可以并行或独立的方式来执行。另外，这里所述的系统是多个设备的逻辑复杂配置，具有各种配置的设备不必设置在同一壳体中。

[0736] 本发明包括与 2011 年 11 月 17 日提交日本专利局的日本优先权专利申请 JP2011-251733 中公开的主题有关的主题，其全部内容通过引用的方式合并在本文本中。

[0737] 本领域的普通技术人员应当理解的是，可根据设计要求和其它因素进行各种修改、组合、子组合和替换，这些均随附权利要求或其等同方案的范围内。


内容记录
介质
31
图1C
用户装置
内容记录和再现设备
(主机)
21
22
23
图1B
内容提供方
11
12
图1A

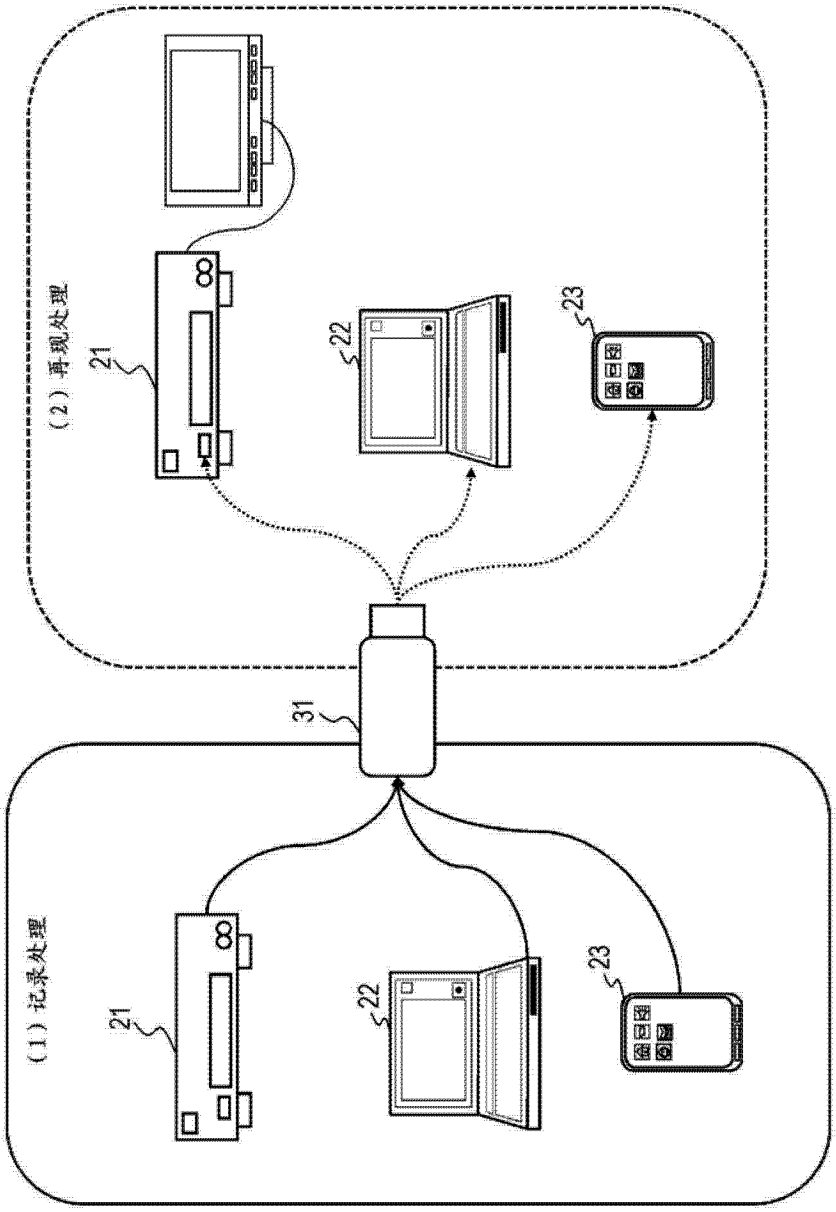


图 2

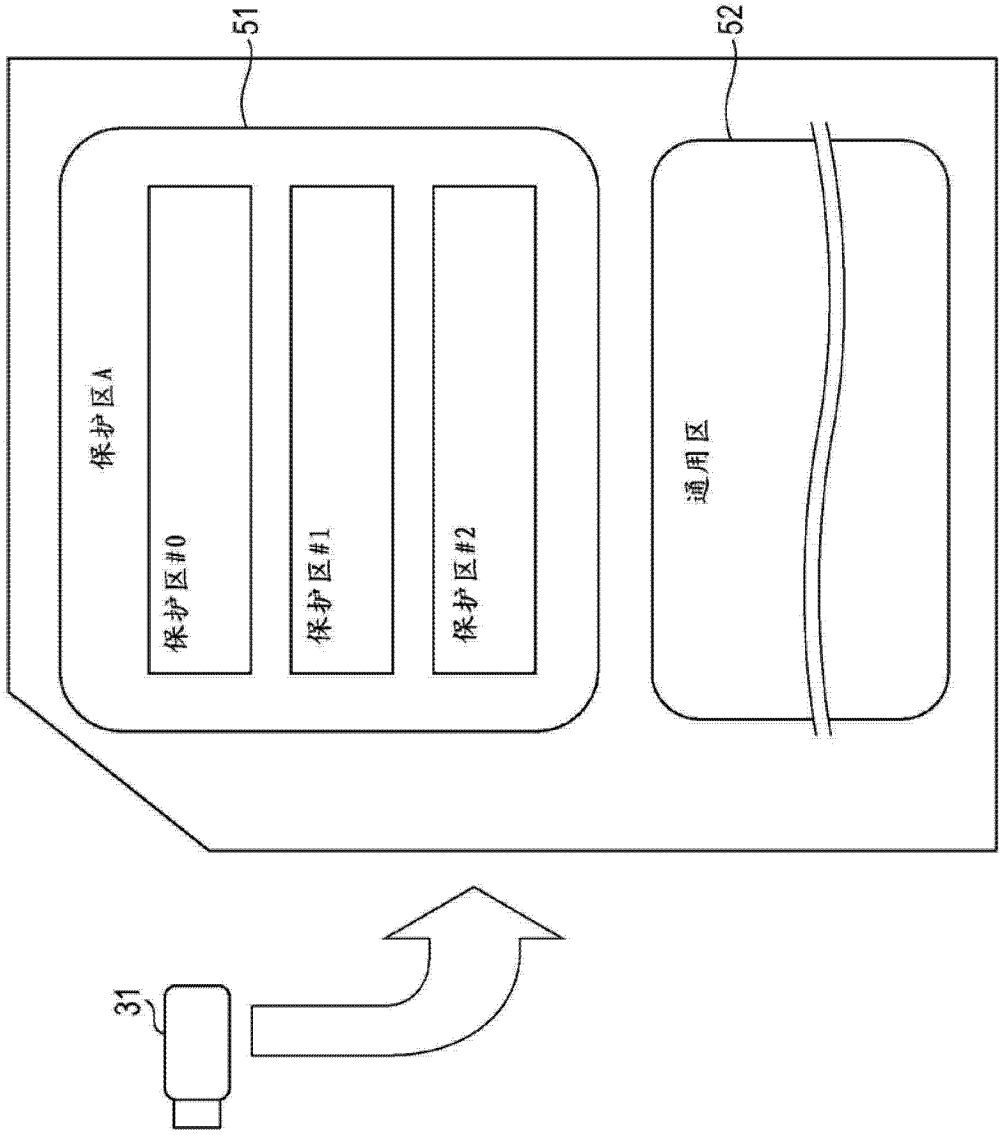


图 3

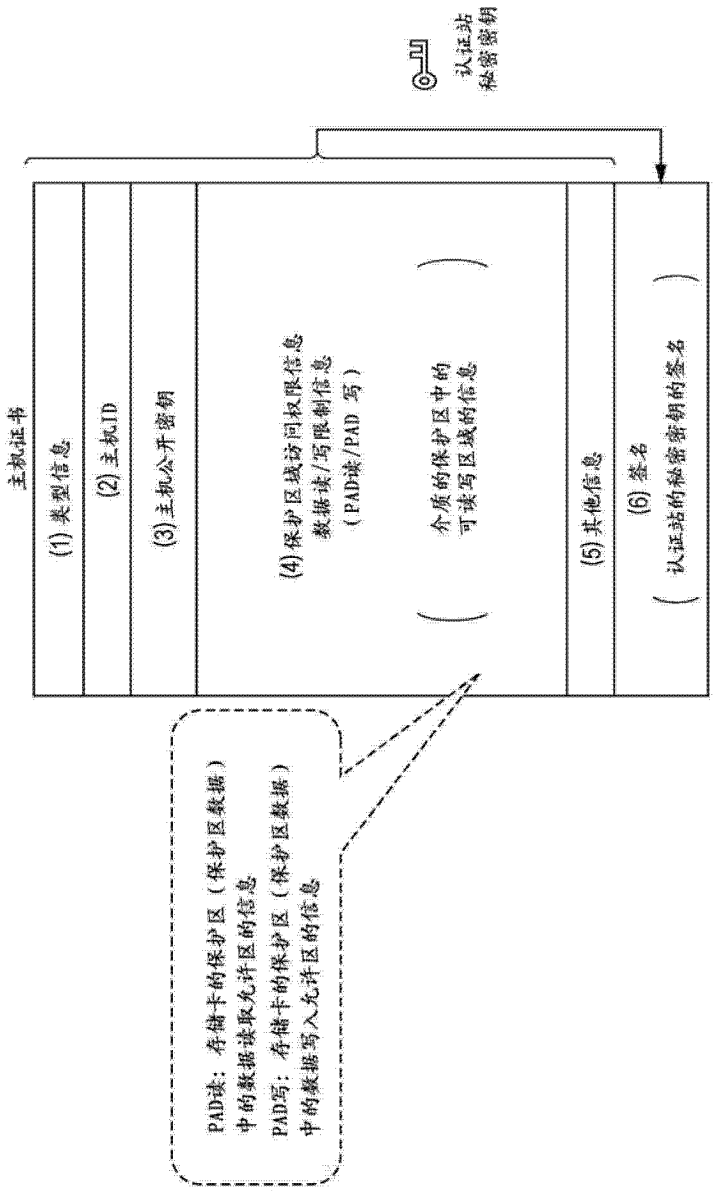

认证站
私密密钥
主机证书
(1) 类型信息
(2) 主机ID
(3) 主机公开密钥
(4) 保护区域访问权限信息
数据读/写限制信息
(PAD读/PAD 写)
介质的保护区中的
可读写区域的信息
(5) 其他信息
(6) 签名
认证站的私密密钥的签名
PAD读：存储卡的保护区（保护区数据）
中的数据读取允许区的信息
PAD写：存储卡的保护区（保护区数据）
中的数据写入允许区的信息

图 4

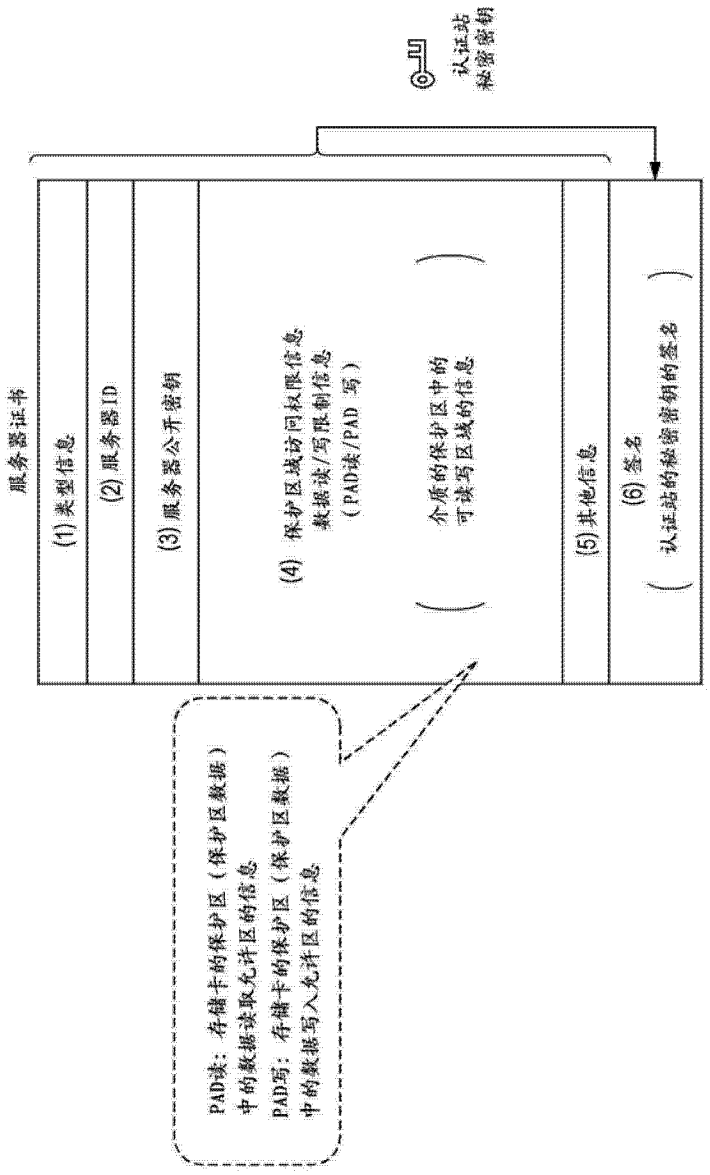

认证站
秘密密钥
服务器证书
(1) 类型信息
(2) 服务器ID
(3) 服务器公开密钥
(4) 保护区域访问权限信息
数据读/写限制信息
(PAD读/PAD 写)
介质的保护区中的
可读写区域的信息
(5) 其他信息
(6) 签名
认证站的秘密密钥的签名
PAD读：存储卡的保护区（保护区数据）
中的数据读取允许区的信息
PAD写：存储卡的保护区（保护区数据）
中的数据写入允许区的信息

图 5

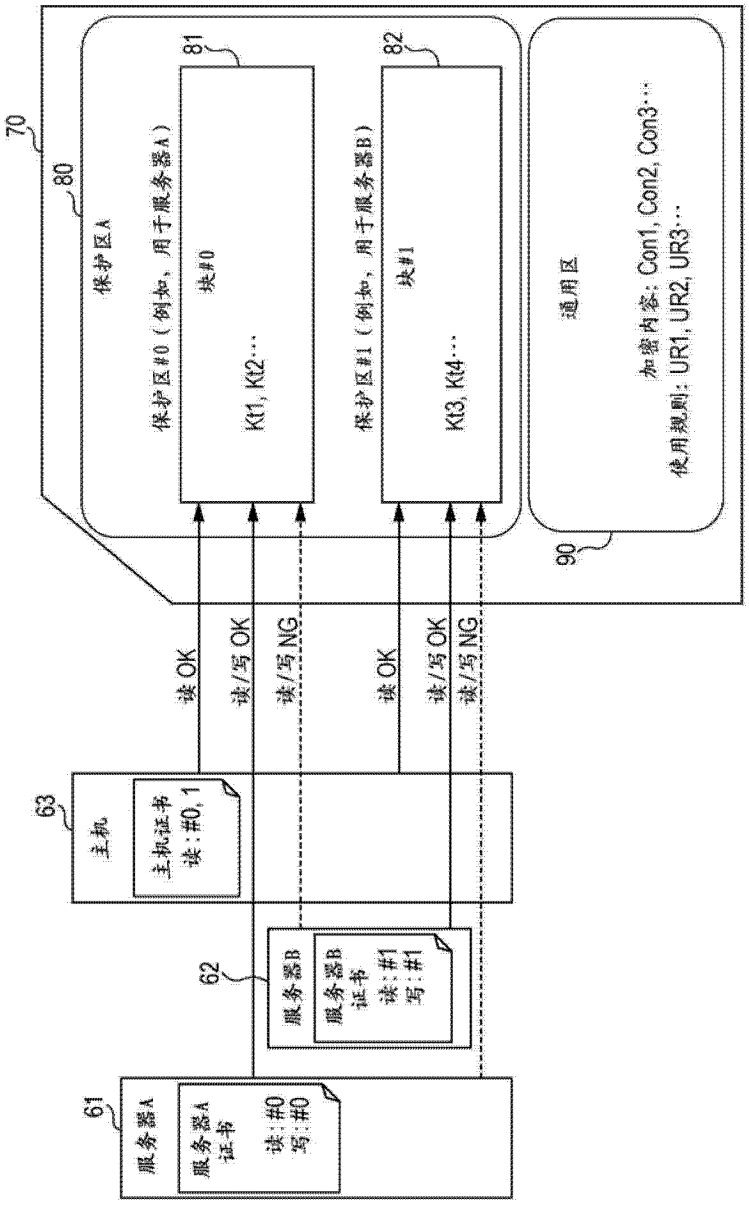

70
80
保护区A
保护区#0（例如，用于服务器A）
81
块#0
Kt1, Kt2…
保护区#1（例如，用于服务器B）
82
块#1
Kt3, Kt4…
通用区
加密内容：Con1, Con2, Con3…
使用规则：UR1, UR2, UR3…
90
读 OK
读/写 OK
读/写 NG
读 OK
读/写 OK
读/写 NG
63
主机
主机证书
读：#0, 1
62
服务器B
服务器B
证书
读：#1
写：#1
61
服务器A
服务器A
证书
读：#0
写：#0

图 6

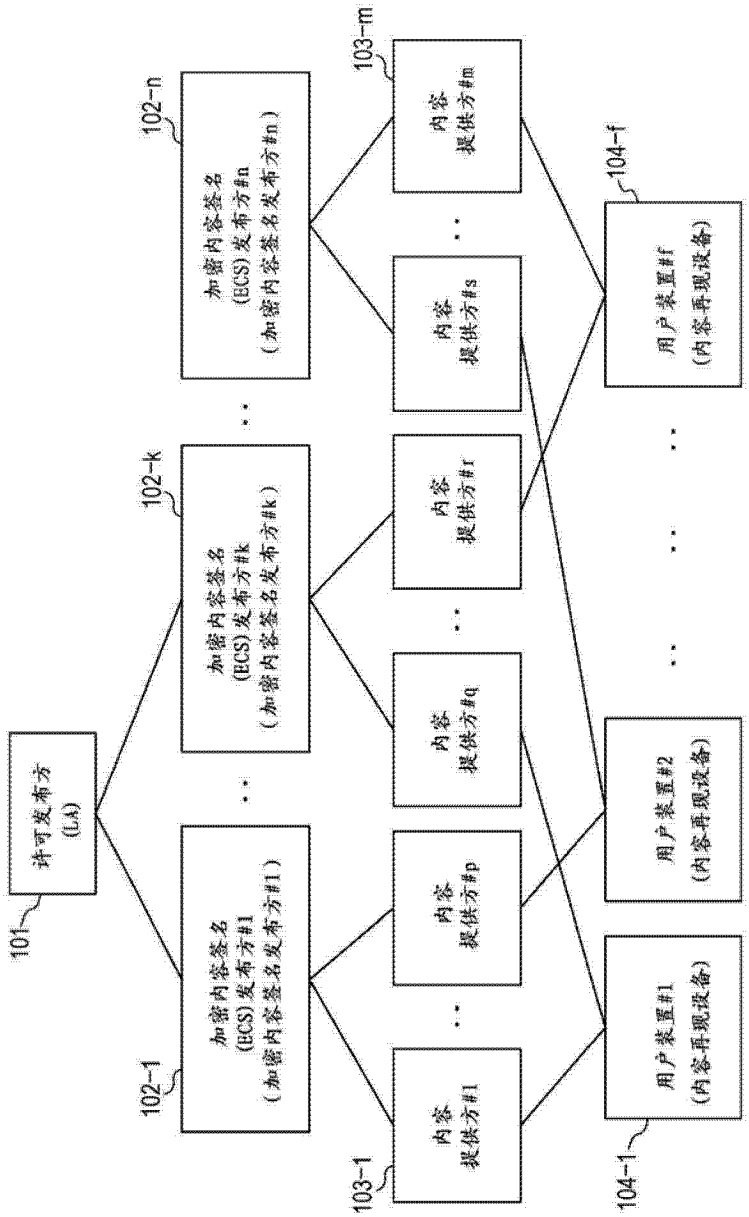

许可发布方
(LA)
101
加密内容签名
(ECS)发布方#1
(加密内容签名发布方#1)
102-1
加密内容签名
(ECS)发布方#k
(加密内容签名发布方#k)
102-k
加密内容签名
(ECS)发布方#n
(加密内容签名发布方#n)
102-n
内容
提供方#1
103-1
内容
提供方#p
内容
提供方#q
内容
提供方#r
内容
提供方#s
内容
提供方#m
103-m
用户装置#1
(内容再现设备)
104-1
用户装置#2
(内容再现设备)
用户装置#f
(内容再现设备)
104-f

图 7

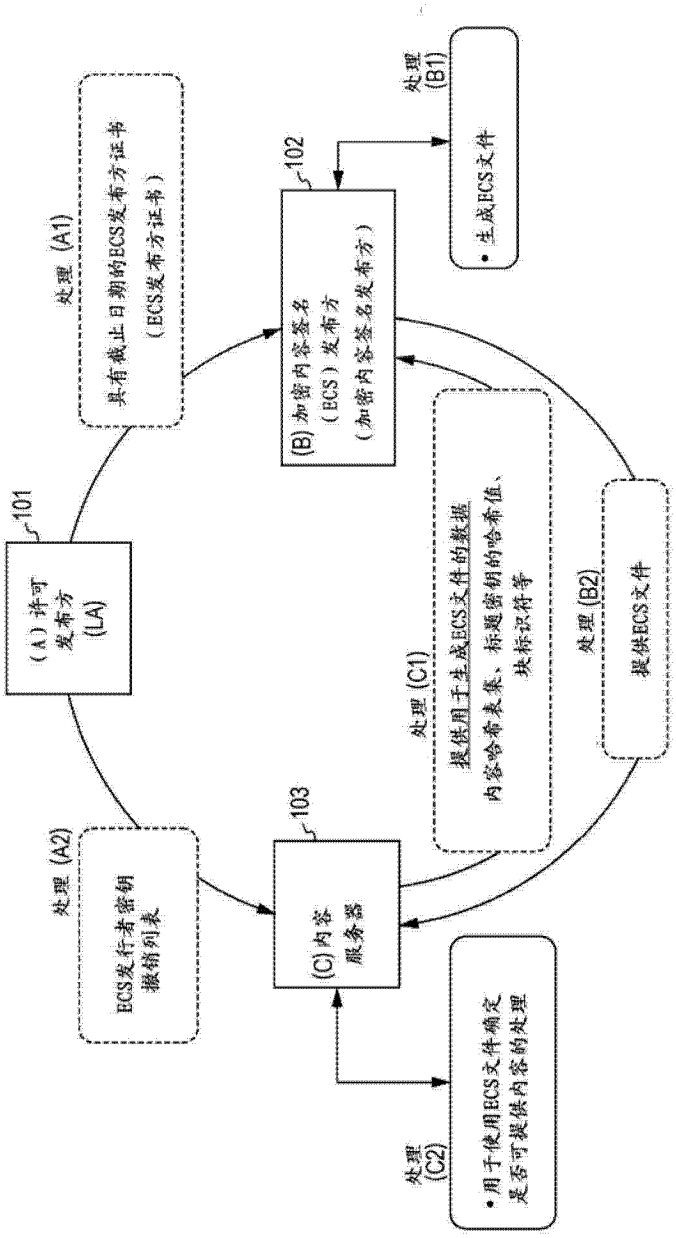

处理 (A1)
具有截止日期的ECS发布方证书
（ECS发布方证书）
101
（A）许可
发布方
(LA)
处理 (A2)
ECS发行者密钥
撤销列表
102
(B) 加密内容签名
（ECS）发布方
（加密内容签名发布方）
处理
(B1)
• 生成ECS文件
处理 (C1)
提供用于生成ECS文件的数据
内容哈希表集、标题密钥的哈希值、
块标识符等
处理 (B2)
提供ECS文件
103
(C) 内容
服务器
处理
(C2)
• 用于使用ECS文件确定
是否可提供内容的处理

图 8

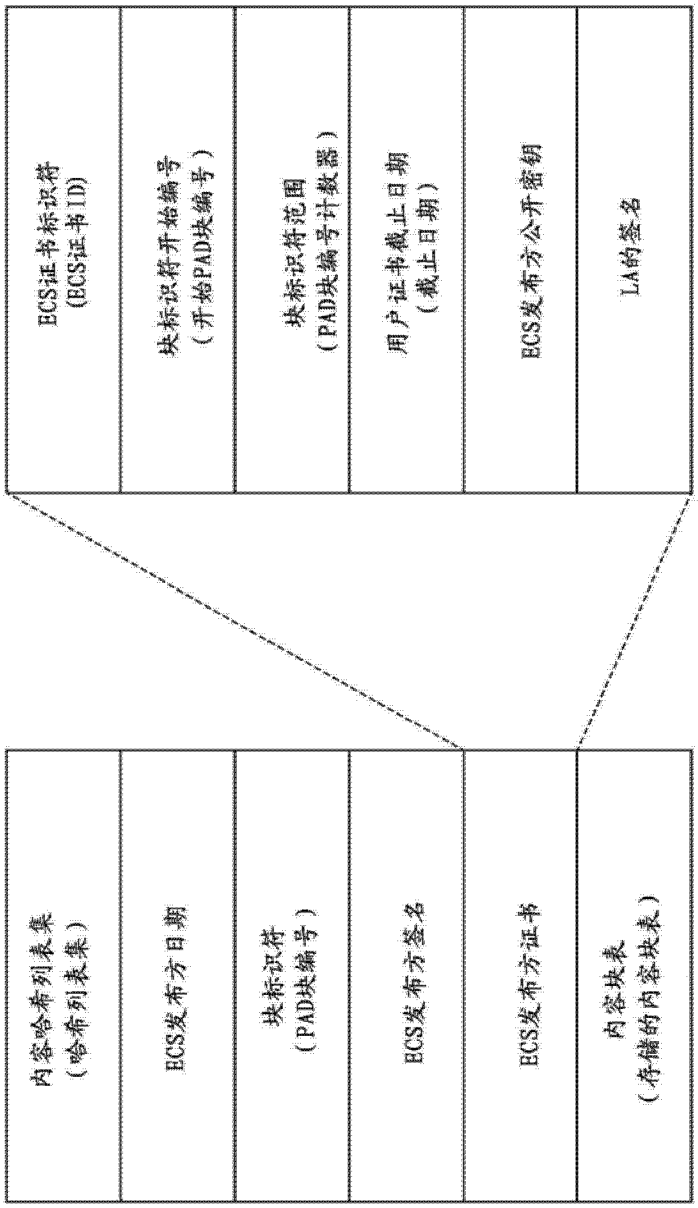

内容哈希列表集
（哈希列表集）
ECS发布方日期
块标识符
（PAD块编号）
ECS发布方签名
ECS发布方证书
内容块表
（存储的内容块表）
ECS证书标识符
(ECS证书ID)
块标识符开始编号
（开始PAD块编号）
块标识符范围
（PAD块编号计数器）
用户证书截止日期
（截止日期）
ECS发布方公开密钥
LA的签名

图9A 图9B

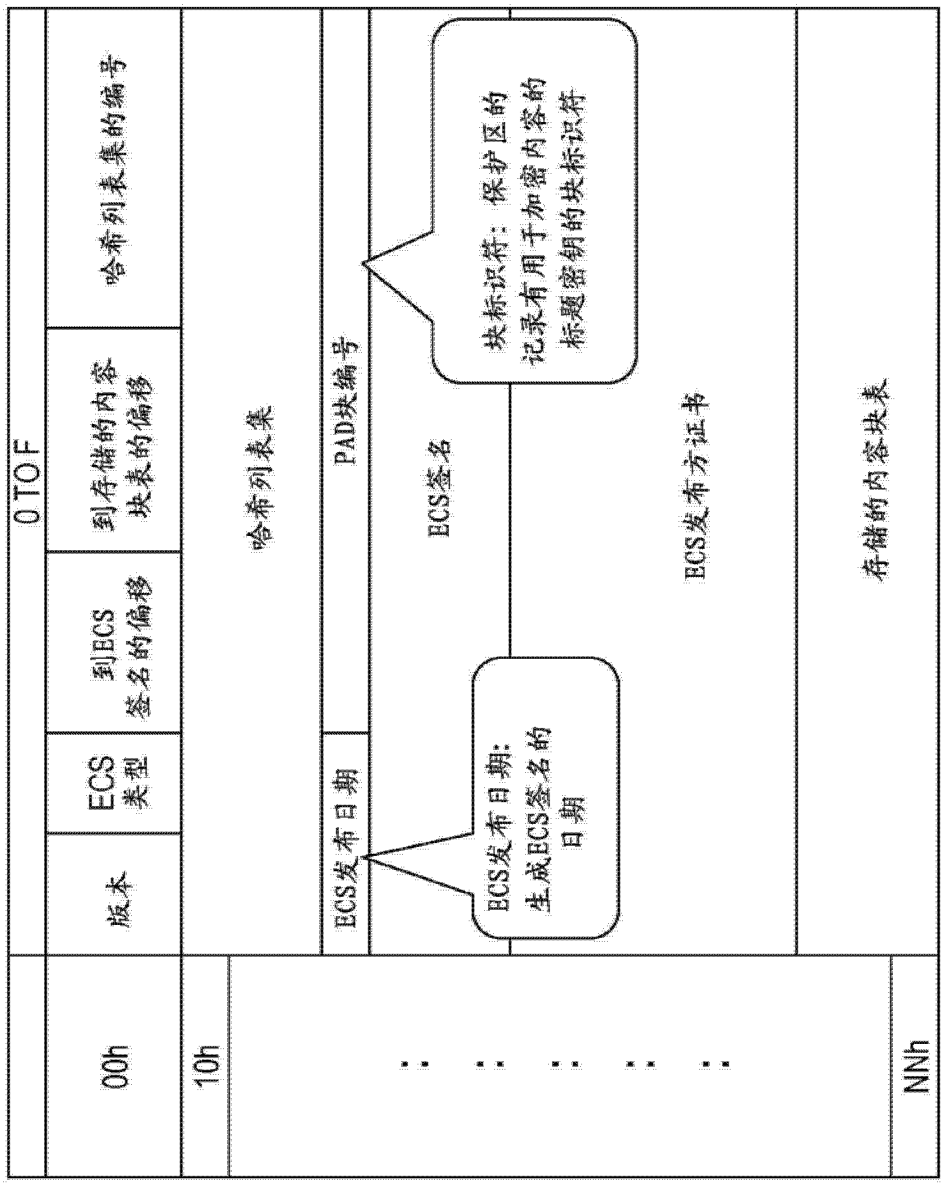

00h
10h
NNh
0 TO F
版本
ECS 类型
到ECS 签名的偏移
到存储的内容 块表的偏移
哈希列表集的编号
哈希列表集
ECS发布日期
PAD块编号
ECS签名
ECS发布方证书
存储的内容块表
ECS发布日期: 生成ECS签名的 日期
块标识符: 保护区的 记录有用于加密内容的 标题密钥的块标识符

图 10

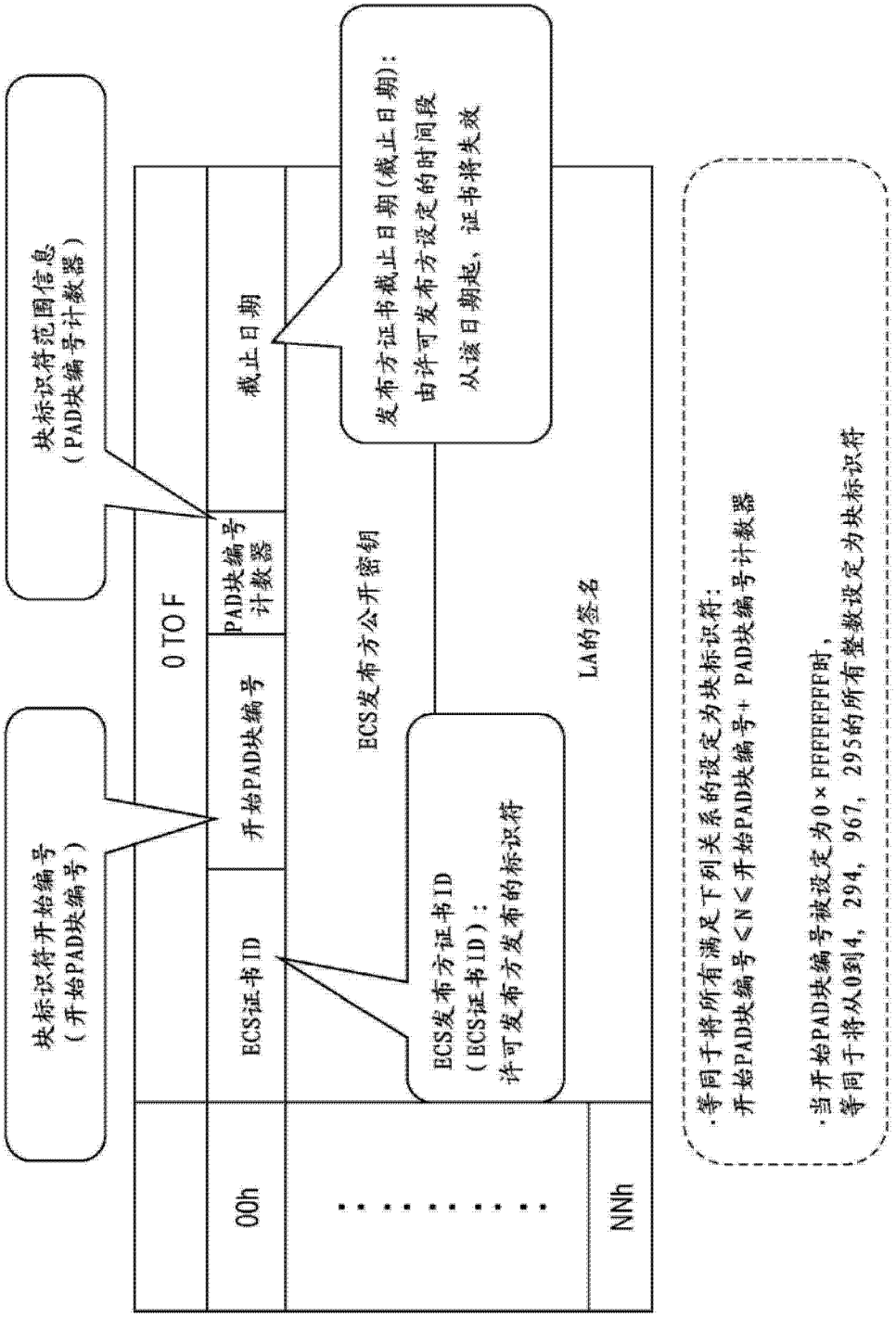

块标识符开始编号
（开始PAD块编号）
块标识符范围信息
（PAD块编号计数器）
发布方证书截止日期(截止日期)：
由许可发布方设定的时间段
从该日期起，证书将失效
0TOF
ECS证书ID
开始PAD块编号
PAD块编号
计数器
截止日期
ECS发布方公开密钥
ECS发布方证书ID
（ECS证书ID）：
许可发布方发布的标识符
LA的签名
00h
NNh
·等同于将所有满足下列关系的设定为块标识符：
开始PAD块编号≤N≤开始PAD块编号+ PAD块编号计数器
·当开始PAD块编号被设定为0×FFFFFFFF时，
等同于将从0到4，294，967，295的所有整数设定为块标识符

图 11

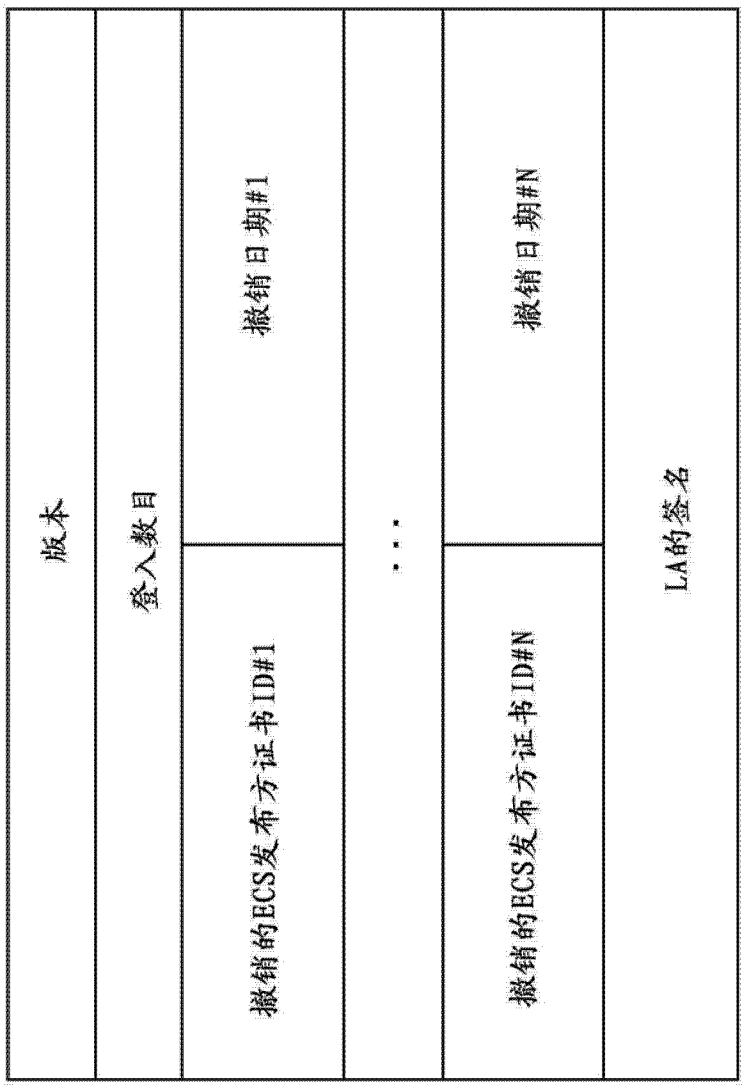


图 12

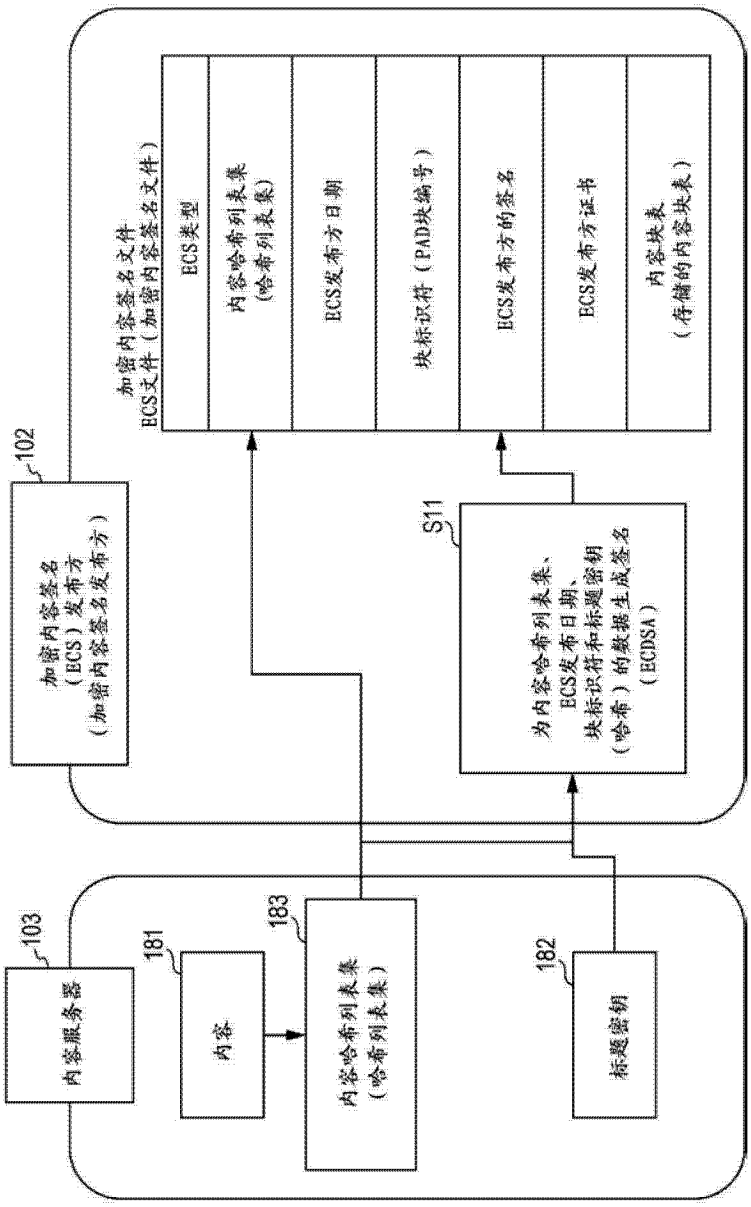

加密内容签名文件
ECS文件（加密内容签名文件）
ECS类型
内容哈希列表集
（哈希列表集）
ECS发布方日期
块标识符（PAD块编号）
ECS发布方的签名
ECS发布方证书
内容块表
（存储的内容块表）
102
加密内容签名
（ECS）发布方
（加密内容签名发布方）
S11
为内容哈希列表集、
ECS发布日期、
块标识符和标题密钥
（哈希）的数据生成签名
（ECDSA）
103
内容服务器
181
内容
183
内容哈希列表集
（哈希列表集）
182
标题密钥

图 13

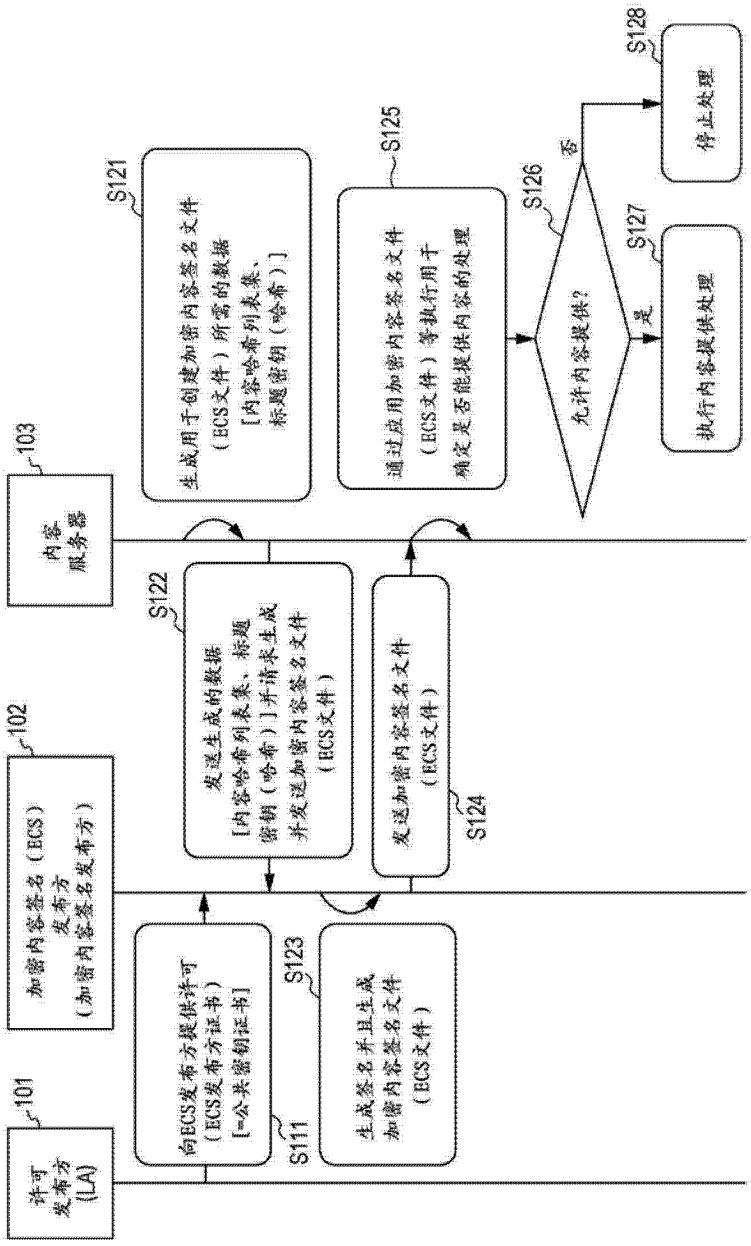

101
许可发布方(LA)
102
加密内容签名(ECS)发布方(加密内容签名发布方)
103
内容服务器
向ECS发布方提供许可(ECS发布方证书)[=公共密钥证书]
S111
生成签名并且生成加密内容签名文件(ECS文件)
S123
发送生成的数据[内容哈希列表集、标题密钥(哈希)]并请求生成并发送加密内容签名文件(ECS文件)
S122
发送加密内容签名文件(ECS文件)
S124
生成用于创建加密内容签名文件(ECS文件)所需的数据[内容哈希列表集、标题密钥(哈希)]
S121
通过应用加密内容签名文件(ECS文件)等执行用于确定是否能提供内容的处理
S125
允许内容提供?
S126
否
是
S127
执行内容提供处理
停止处理
S128

图 14

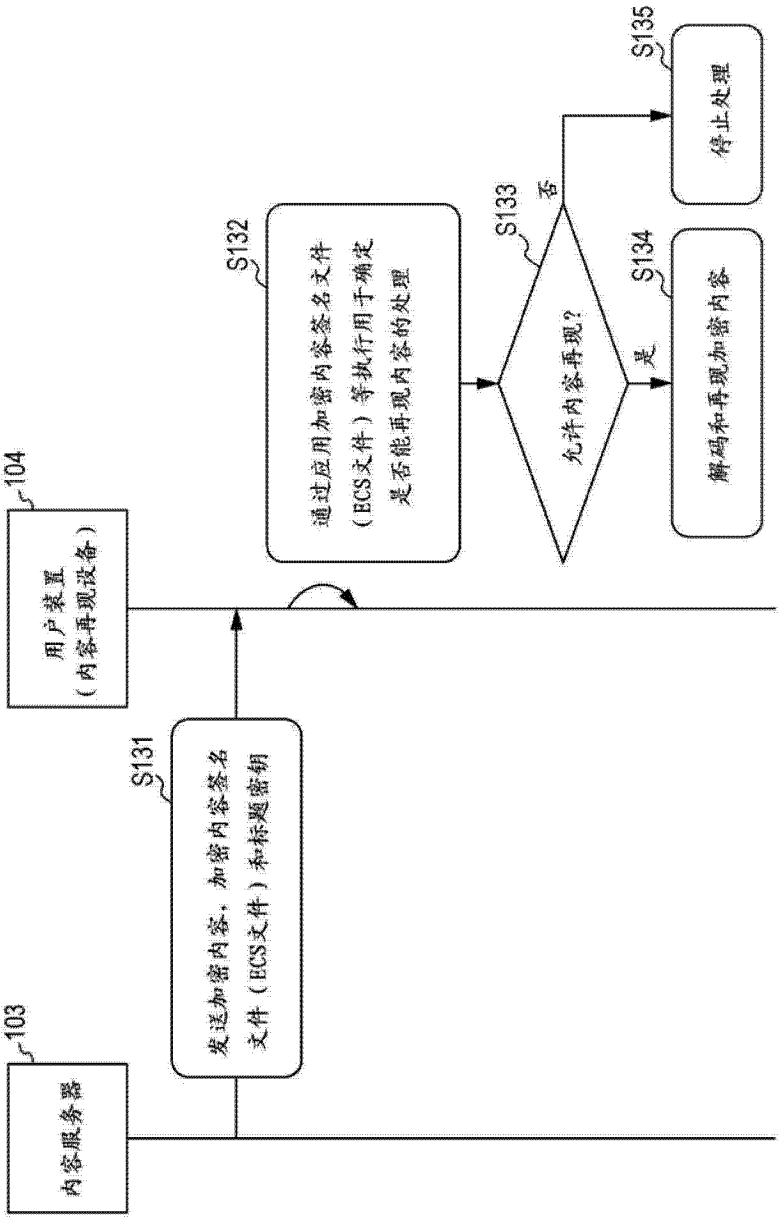

103
内容服务器
104
用户装置
（内容再现设备）
S131
发送加密内容，加密内容签名文件（ECCS文件）和标题密钥
S132
通过应用加密内容签名文件（ECCS文件）等执行用于确定是否能再现内容的处理
S133
允许内容再现?
否
是
S134
解码和再现加密内容
S135
停止处理

图 15

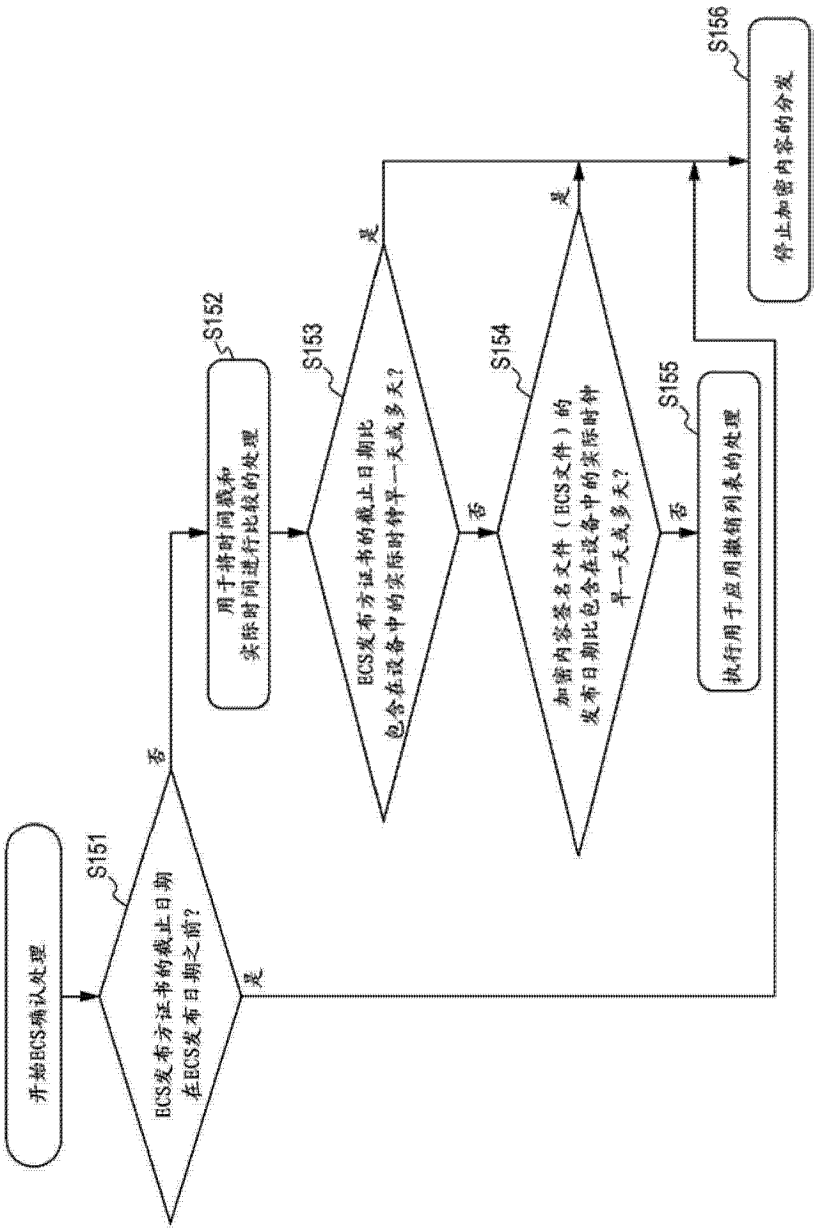

开始ECS确认处理
S151
ECS发布方证书的截止日期在ECS发布日期之前?
否
是
S152
用于将时间戳和实际时间进行比较的处理
S153
ECS发布方证书的截止日期比包含在设备中的实际时钟早一天或多天?
否
是
S154
加密内容签名文件(ECS文件)的发布日期比包含在设备中的实际时钟早一天或多天?
否
是
S155
执行用于应用撤销列表的处理
S156
停止加密内容的分发

图 16

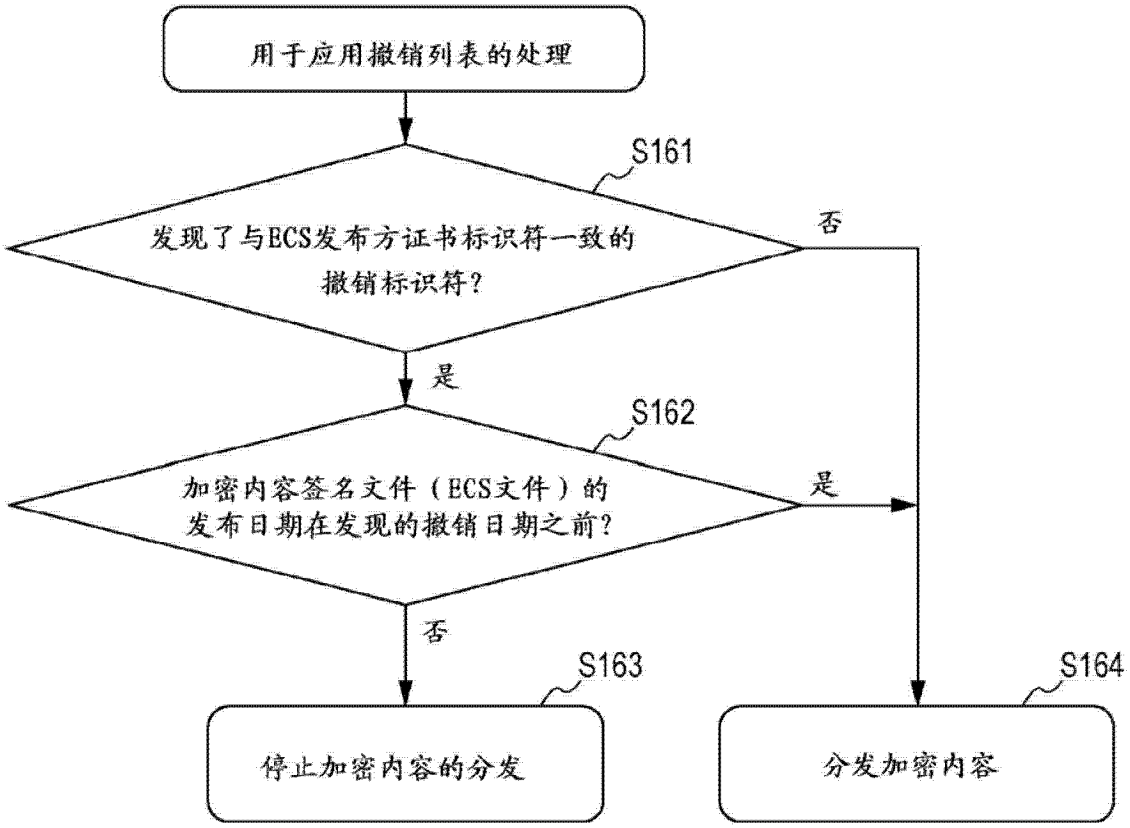

用于应用撤销列表的处理
S161
发现了与ECS发布方证书标识符一致的撤销标识符？
否
是
S162
加密内容签名文件（ECS文件）的发布日期在发现的撤销日期之前？
是
否
S163
停止加密内容的分发
S164
分发加密内容

图 17

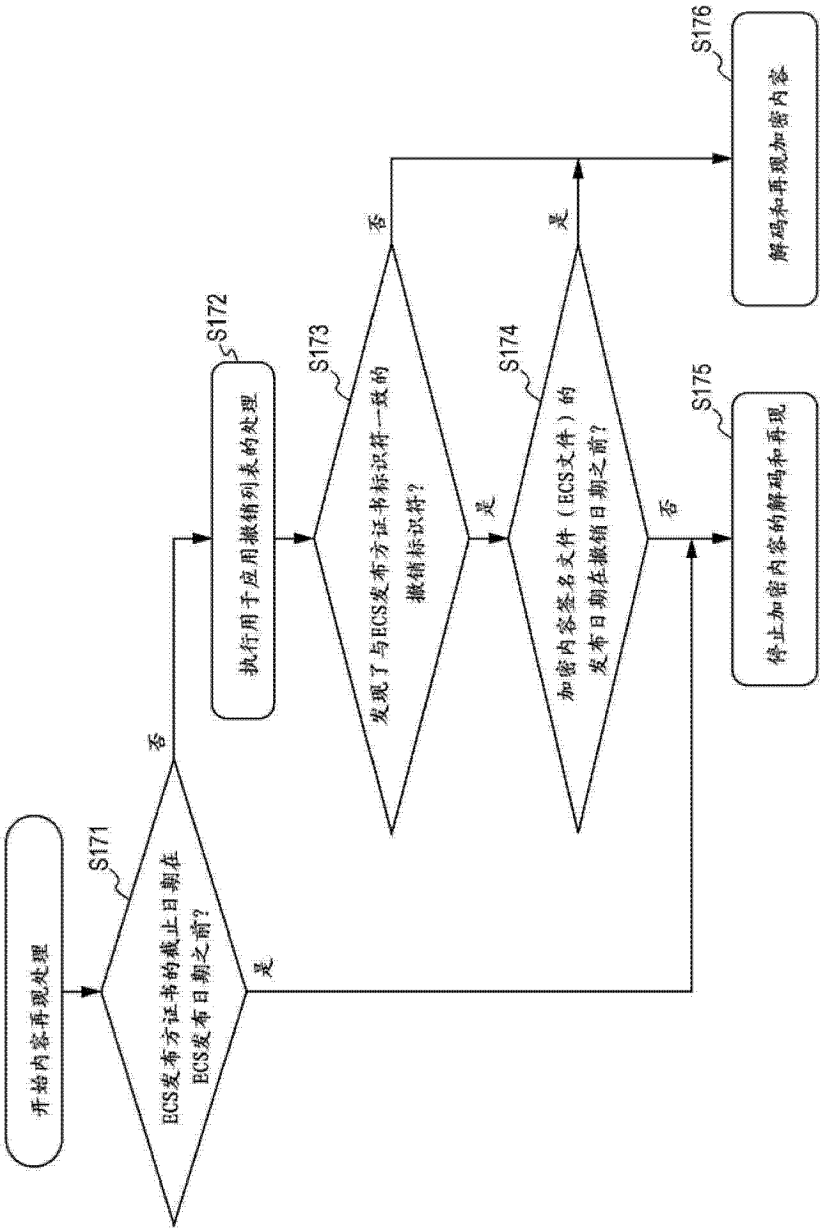

开始内容再现处理
S171
ECS发布方证书的截止日期在ECS发布日期之前?
否
是
S172
执行用于应用撤销列表的处理
S173
发现了与ECS发布方证书标识符一致的撤销标识符?
否
是
S174
加密内容签名文件（ECS文件）的发布日期在撤销日期之前?
否
是
S175
停止加密内容的解码和再现
S176
解码和再现加密内容

图 18

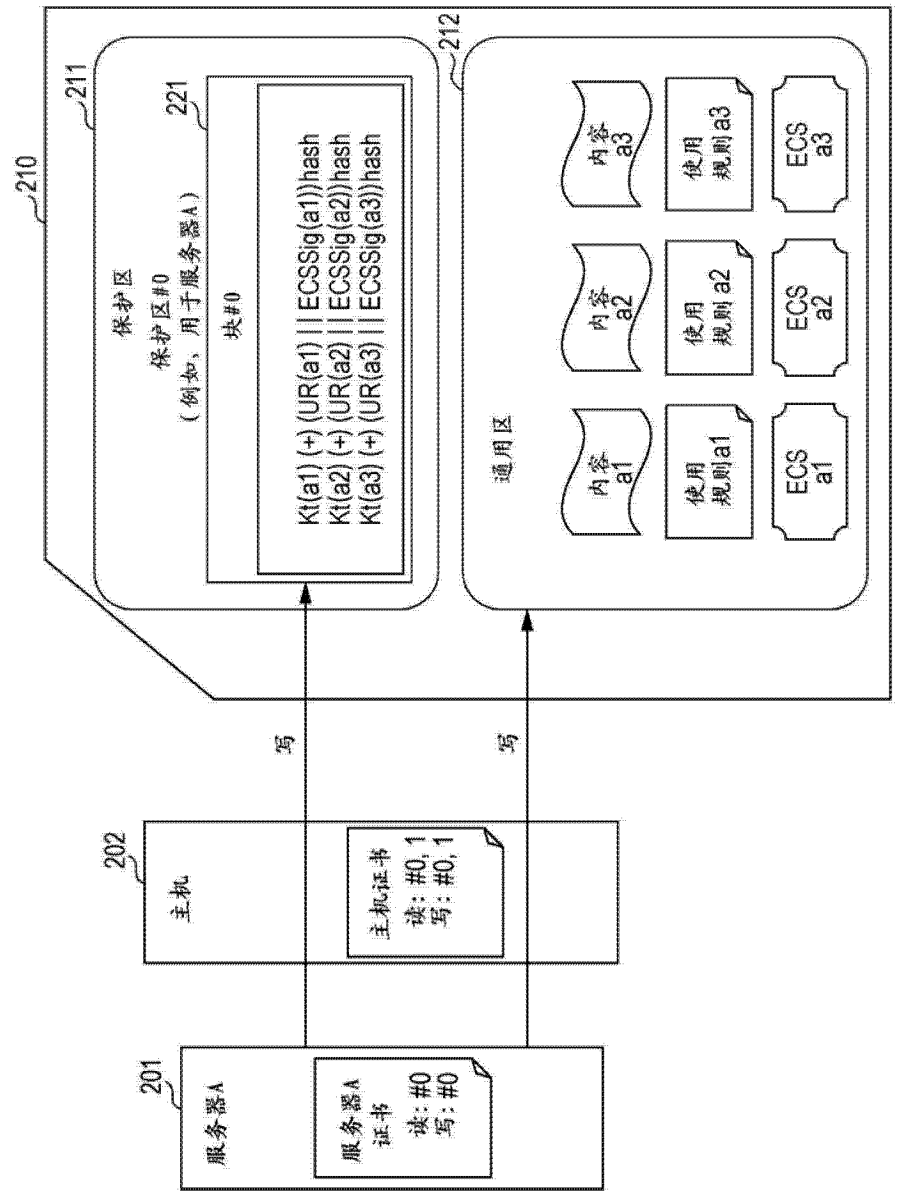

210
211
保护区
保护区#0
（例如，用于服务器A）
221
块#0
Kt(a1) (+) (UR(a1) || ECSSig(a1))hash
Kt(a2) (+) (UR(a2) || ECSSig(a2))hash
Kt(a3) (+) (UR(a3) || ECSSig(a3))hash
212
通用区
内容 a1
使用规则a1
ECS a1
内容 a2
使用规则 a2
ECS a2
内容 a3
使用规则a3
ECS a3
写
写
202
主机
主机证书
读：#0, 1
写：#0, 1
201
服务器A
服务器A证书
读：#0
写：#0

图 19

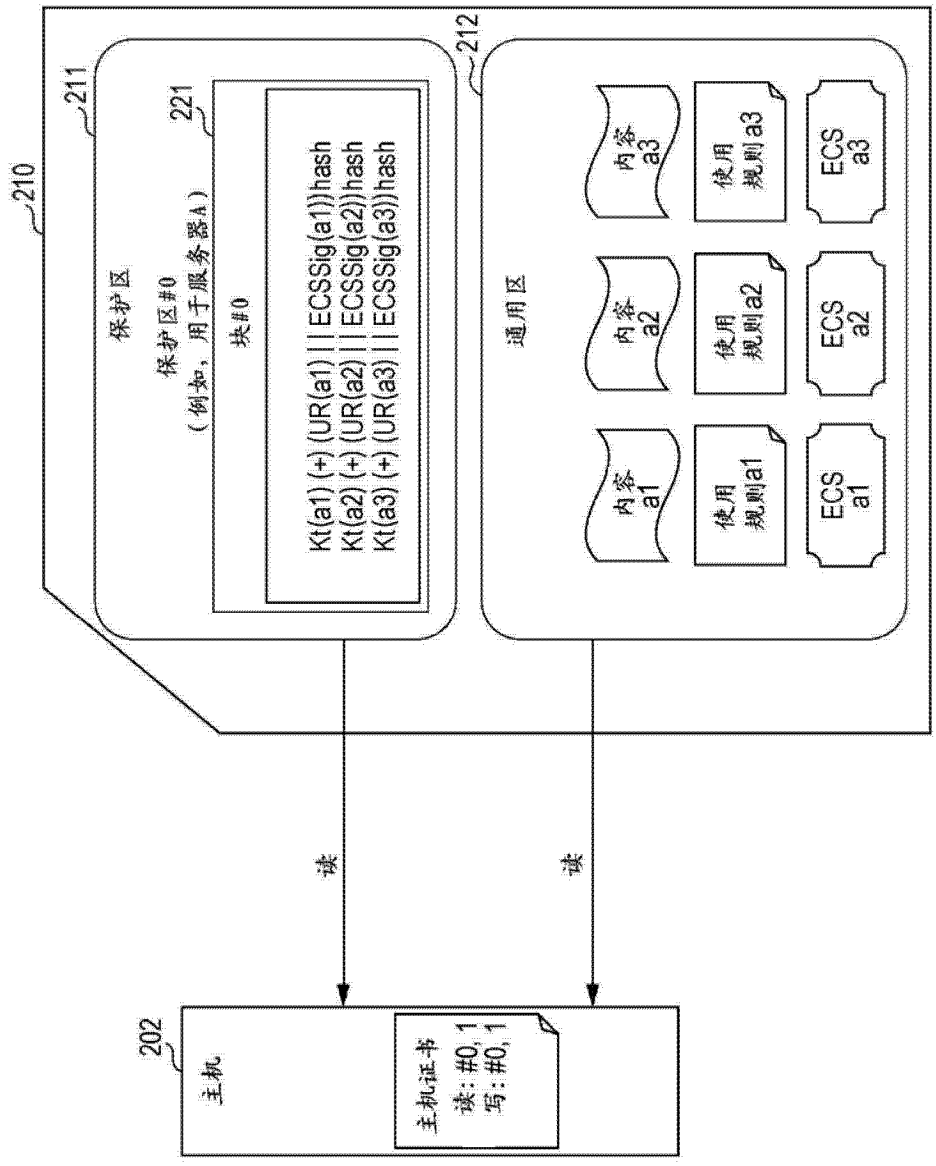
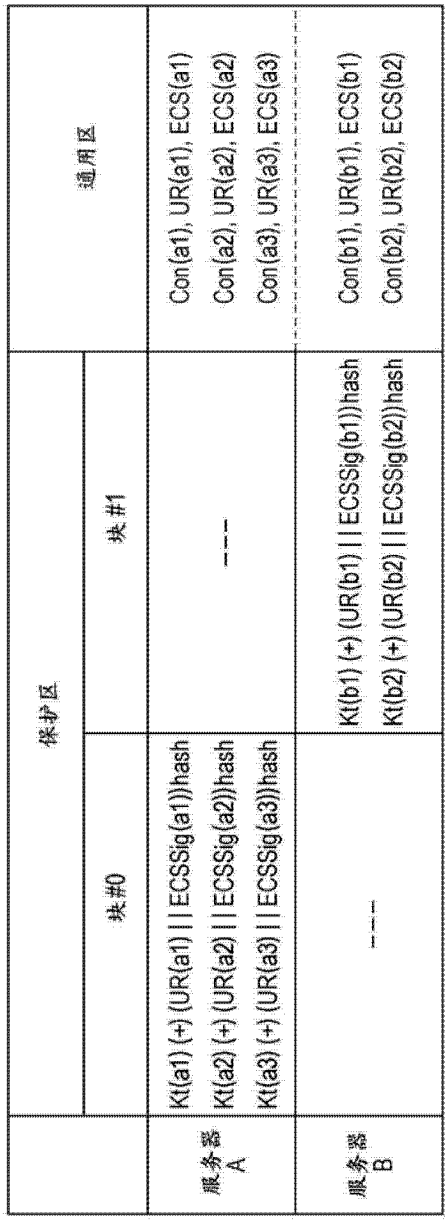
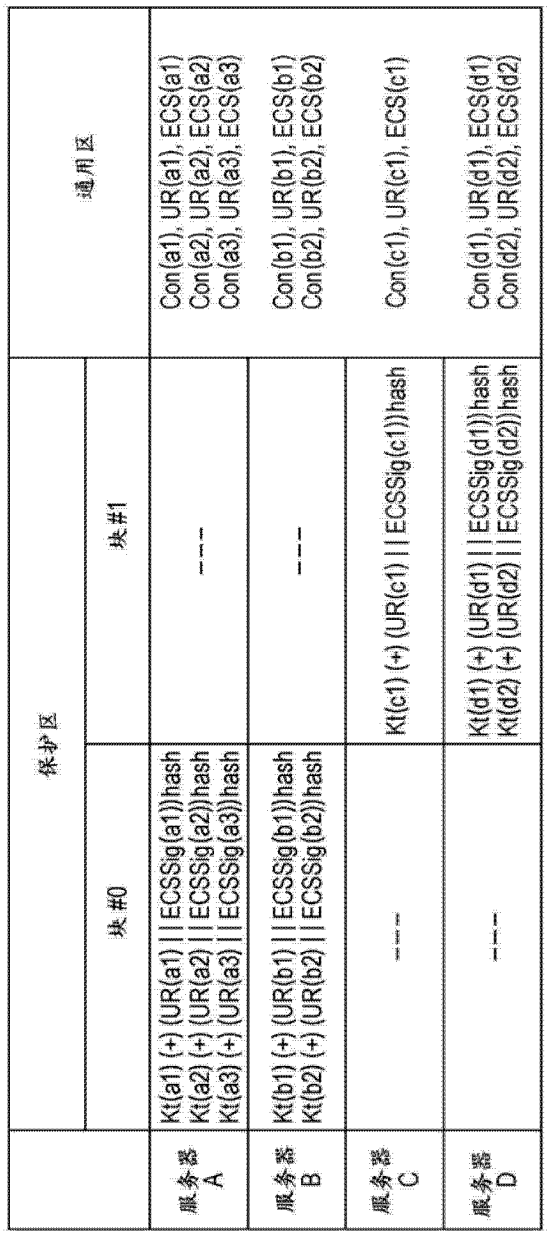

210
211
保护区
保护区#0
（例如，用于服务器A）
221
块#0
Kt(a1) (+) (UR(a1) || ECSSig(a1))hash
Kt(a2) (+) (UR(a2) || ECSSig(a2))hash
Kt(a3) (+) (UR(a3) || ECSSig(a3))hash
212
通用区
内容 a3
使用规则a3
ECS a3
内容 a2
使用规则a2
ECS a2
内容 a1
使用规则a1
ECS a1
读
读
202
主机
主机证书
读：#0, 1
写：#0, 1

图 20



	保护区		通用区
	块#0	块#1	
服务器 A	Kt(a1) (+) (UR(a1) | | ECSSig(a1))hash Kt(a2) (+) (UR(a2) | | ECSSig(a2))hash Kt(a3) (+) (UR(a3) | | ECSSig(a3))hash	---	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
服务器 B	---	Kt(b1) (+) (UR(b1) | | ECSSig(b1))hash Kt(b2) (+) (UR(b2) | | ECSSig(b2))hash	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)

图 21



	保护区		通用区
	块#0	块#1	
服务器 A	Kt(a1) (+) (UR(a1) | | ECSSig(a1))hash Kt(a2) (+) (UR(a2) | | ECSSig(a2))hash Kt(a3) (+) (UR(a3) | | ECSSig(a3))hash	---	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
服务器 B	Kt(b1) (+) (UR(b1) | | ECSSig(b1))hash Kt(b2) (+) (UR(b2) | | ECSSig(b2))hash	---	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)
服务器 C	---	Kt(c1) (+) (UR(c1) | | ECSSig(c1))hash	Con(c1), UR(c1), ECS(c1)
服务器 D	---	Kt(d1) (+) (UR(d1) | | ECSSig(d1))hash Kt(d2) (+) (UR(d2) | | ECSSig(d2))hash	Con(d1), UR(d1), ECS(d1) Con(d2), UR(d2), ECS(d2)

图 22

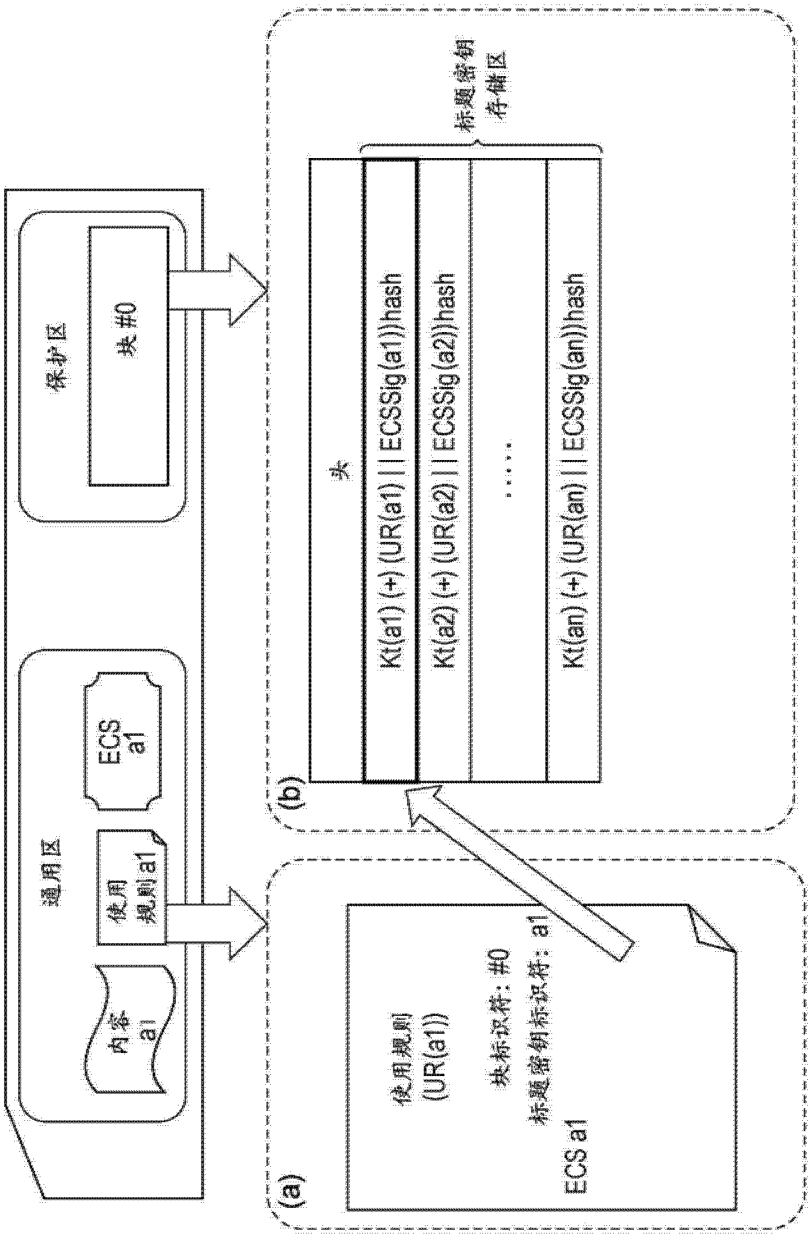

保护区
块 #0
通用区
ECS a1
使用规则 a1
内容 a1
(a)
使用规则 (UR(a1))
块标识符：#0
标题密钥标识符：a1
ECS a1
(b)
头
标题密钥存储区
Kt(a1) (+) (UR(a1) || ECSSig(a1))hash
Kt(a2) (+) (UR(a2) || ECSSig(a2))hash
.....
Kt(an) (+) (UR(an) || ECSSig(an))hash

图 23

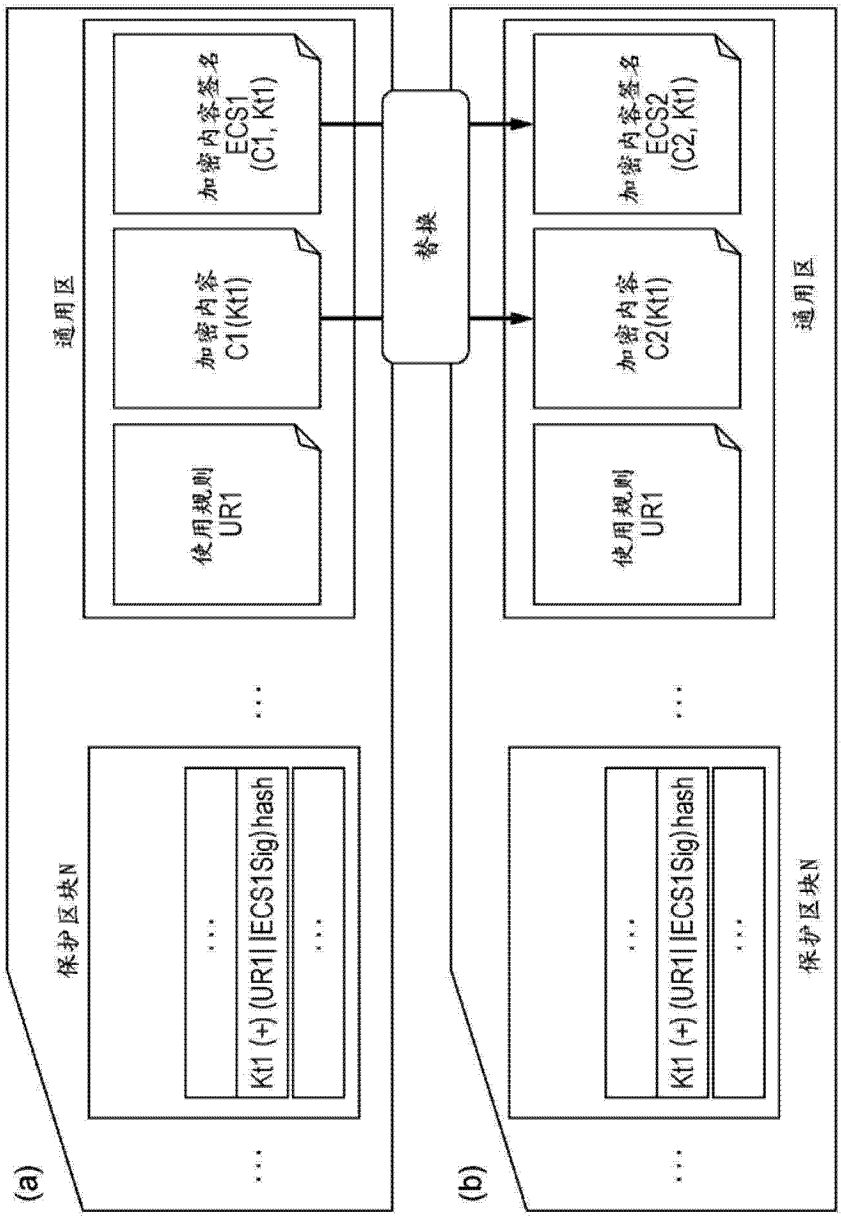

(a)
通用区
使用规则
UR1
加密内容
C1(Kt1)
加密内容签名
ECS1
(C1, Kt1)
保护区块N
Kt1 (+) (UR1||ECS1Sig)hash
替换
(b)
通用区
使用规则
UR1
加密内容
C2(Kt1)
加密内容签名
ECS2
(C2, Kt1)
保护区块N
Kt1 (+) (UR1||ECS1Sig)hash

图 24

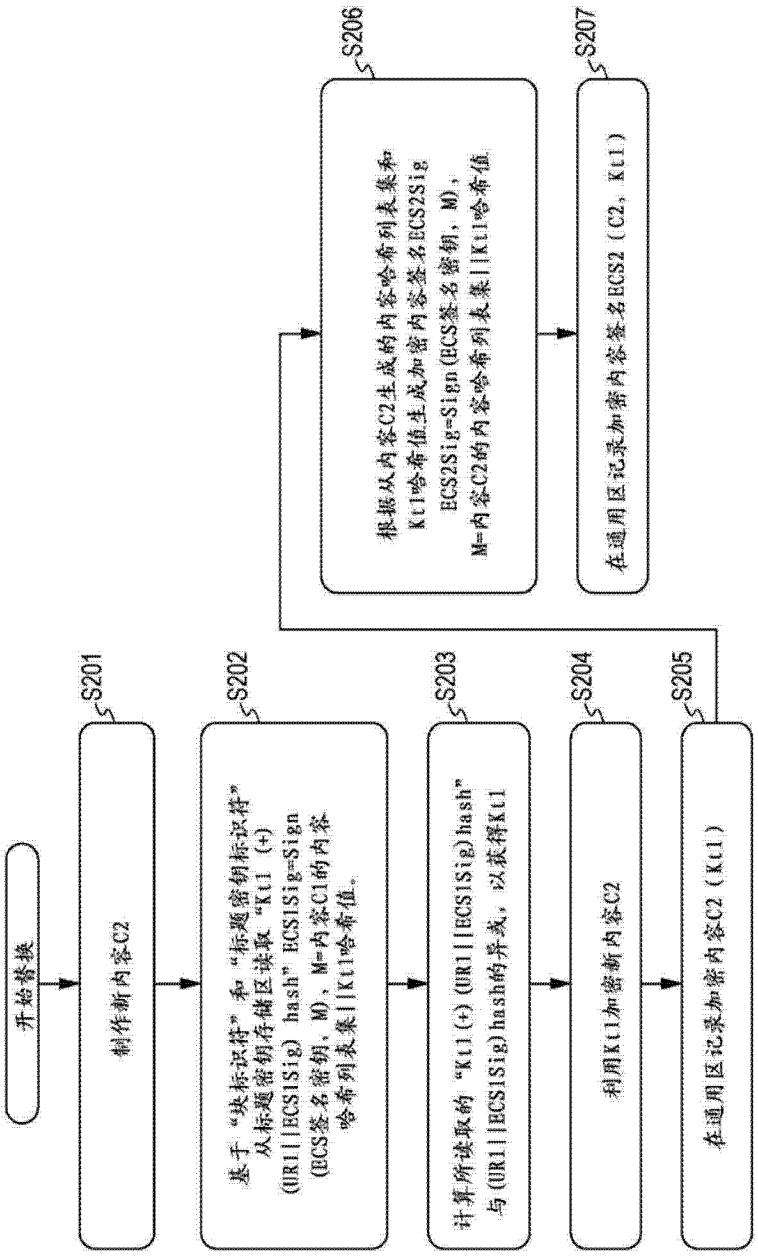

开始替换
S201
制作新内容C2
S202
基于“块标识符”和“标题密钥标识符”从标题密钥存储区读取“Kt1（+）(UR1||ECS1Sig) hash”ECS1Sig=Sign(ECS签名密钥，M)，M=内容C1的内容哈希列表集||Kt1哈希值。
S203
计算所读取的“Kt1（+）(UR1||ECS1Sig)hash”与(UR1||ECS1Sig)hash的异或，以获得Kt1
S204
利用Kt1加密新内容C2
S205
在通用区记录加密内容C2（Kt1）
S206
根据从内容C2生成的内容哈希列表集和Kt1哈希值生成加密内容签名ECS2Sig
ECS2Sig=Sign(ECS签名密钥，M)，
M=内容C2的内容哈希列表集||Kt1哈希值
S207
在通用区记录加密内容签名ECS2（C2，Kt1）

图 25

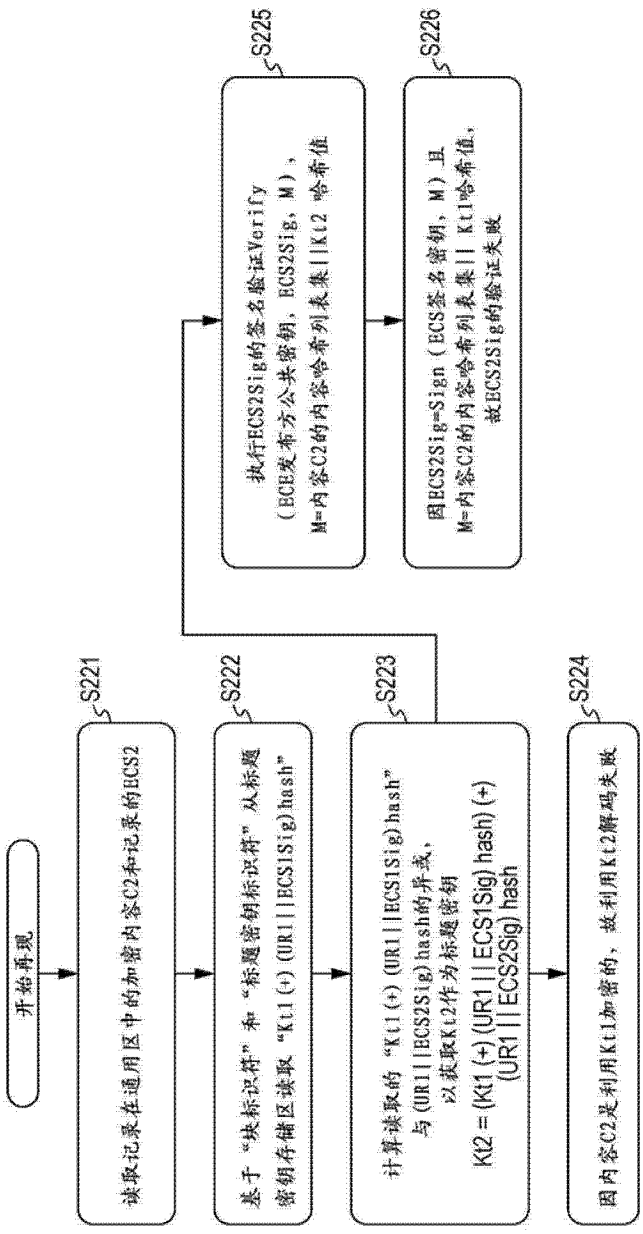

开始再现
S221
读取记录在通用区中的加密内容C2和记录的ECS2
S222
基于“块标识符”和“标题密钥标识符”从标题密钥存储区读取“Kt1(+)(UR1||ECS1Sig)hash”
S223
计算读取的“Kt1(+)(UR1||ECS1Sig)hash”与(UR1||ECS2Sig)hash的异或，以获取Kt2作为标题密钥
Kt2 = (Kt1(+)(UR1||ECS1Sig)hash)(+)(UR1||ECS2Sig)hash
S224
因内容C2是利用Kt1加密的，故利用Kt2解码失败
S225
执行ECS2Sig的签名验证Verify（ECB发布方公共密钥，ECS2Sig，M），M=内容C2的内容哈希列表||Kt2 哈希值
S226
因ECS2Sig=Sign（ECS签名密钥，M）且M=内容C2的内容哈希列表|| Kt1哈希值，故ECS2Sig的验证失败

图 26

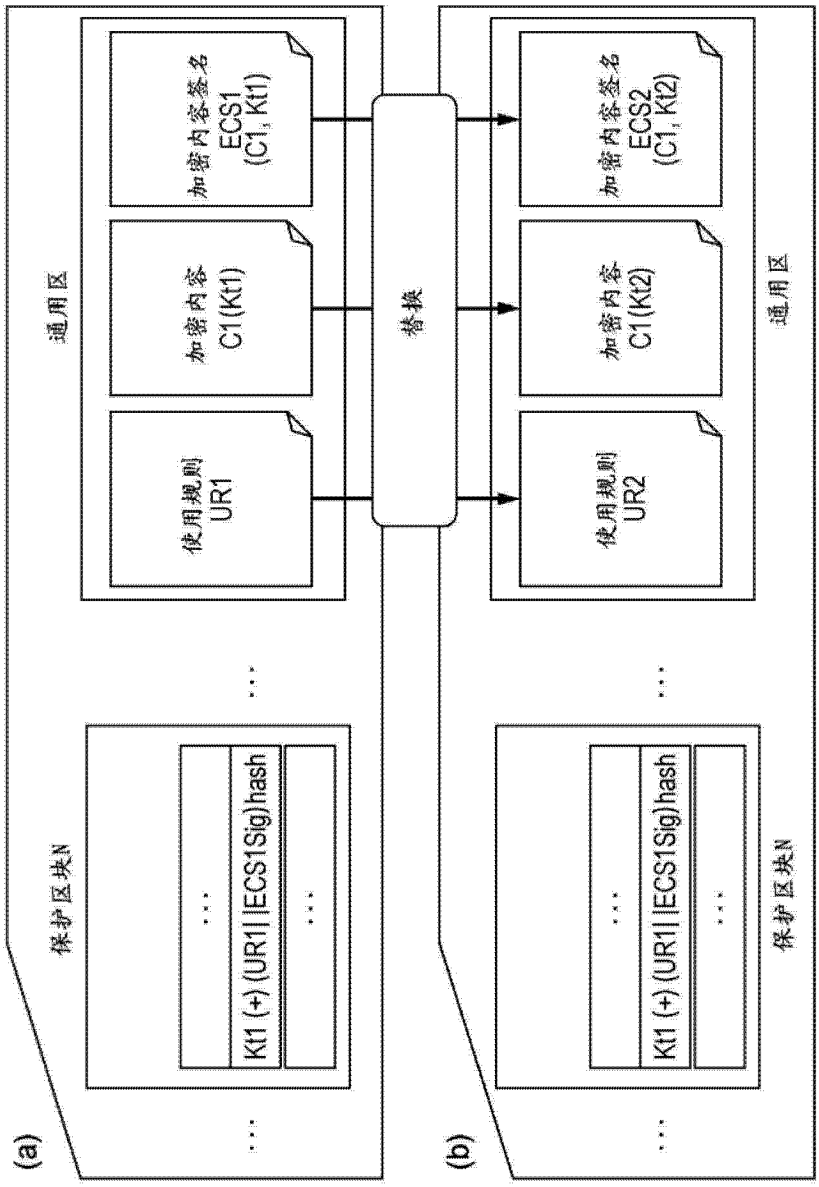

(a)
通用区
加密内容签名
ECS1
(C1, Kt1)
加密内容
C1(Kt1)
使用规则
UR1
保护区块N
Kt1 (+) (UR1||ECS1Sig)hash
替换
(b)
通用区
加密内容签名
ECS2
(C1, Kt2)
加密内容
C1(Kt2)
使用规则
UR2
保护区块N
Kt1 (+) (UR1||ECS1Sig)hash

图 27

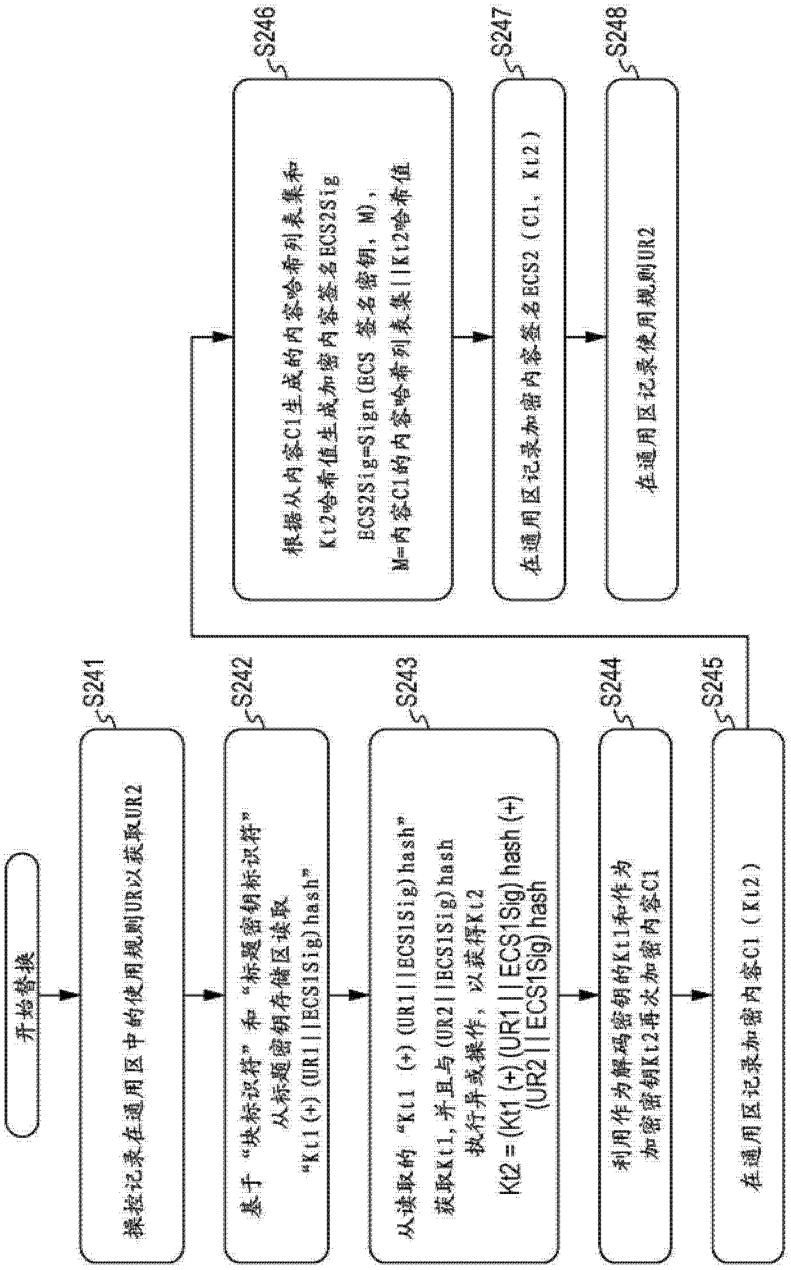

开始替换
S241
操控记录在通用区中的使用规则UR以获取UR2
S242
基于“块标识符”和“标题密钥标识符”
从标题密钥存储区读取
“Kt1(+)(UR1||ECS1Sig)hash”
S243
从读取的“Kt1 (+) (UR1||ECS1Sig)hash”
获取Kt1，并且与(UR2||ECS1Sig)hash
执行异或操作，以获得Kt2
Kt2 = (Kt1 (+) (UR1 || ECS1Sig) hash (+)
(UR2||ECS1Sig) hash
S244
利用作为解码密钥的Kt1和作为
加密密钥Kt2再次加密内容C1
S245
在通用区记录加密内容C1（Kt2）
S246
根据从内容C1生成的内容哈希列表集和
Kt2哈希值生成加密内容签名ECS2Sig
ECS2Sig=Sign(ECS 签名密钥，M)，
M=内容C1的内容哈希列表集||Kt2哈希值
S247
在通用区记录加密内容签名ECS2（C1，Kt2）
S248
在通用区记录使用规则UR2

图 28

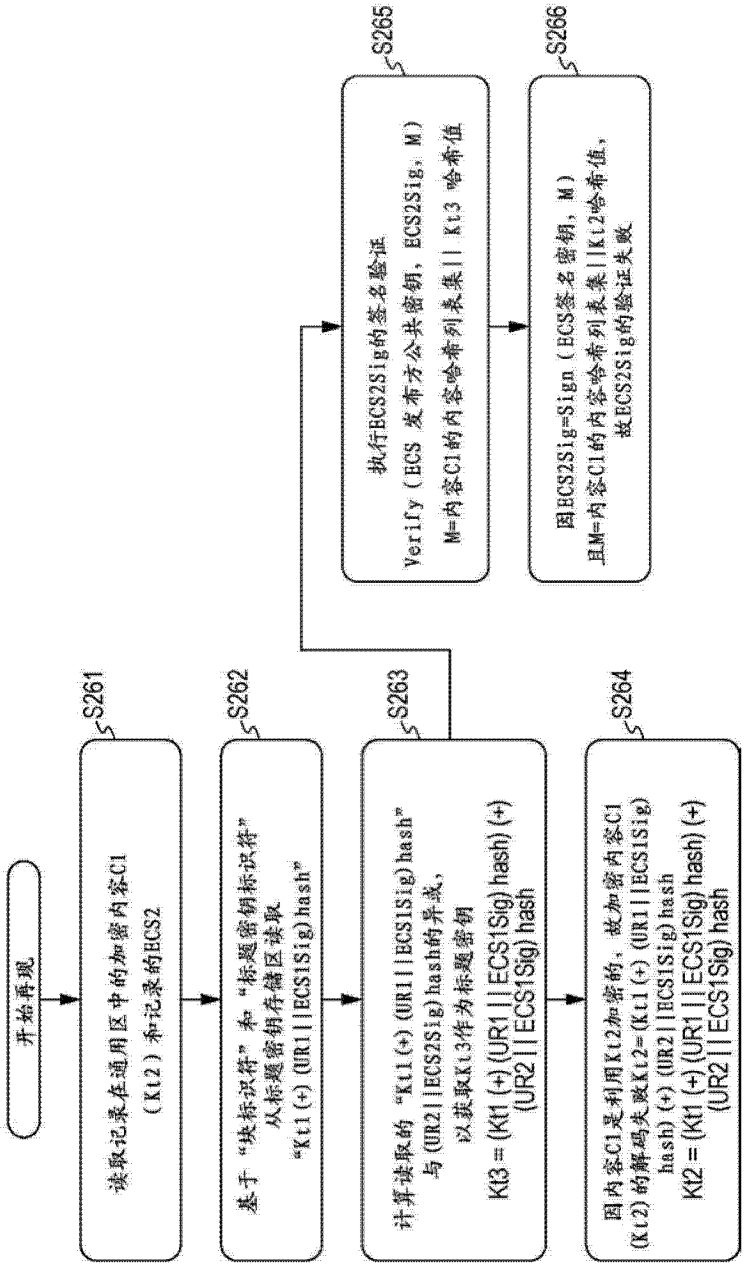

开始再现
S261
读取记录在通用区中的加密内容C1
(Kt2)和记录的ECS2
S262
基于“块标识符”和“标题密钥标识符”
从标题密钥存储区读取
“Kt1(+)(UR1||ECS1Sig)hash”
S263
计算读取的“Kt1(+)(UR1||ECS1Sig)hash”
与(UR2||ECS2Sig)hash的异或，
以获取Kt3作为标题密钥
Kt3 = (Kt1(+)(UR1||ECS1Sig)hash)(+)
(UR2||ECS1Sig)hash
S264
因内容C1是利用Kt2加密的，故加密内容C1
(Kt2)的解码失败Kt2=(Kt1(+)(UR1||ECS1Sig)
hash)(+)(UR2||ECS1Sig)hash
Kt2 = (Kt1(+)(UR1||ECS1Sig)hash)(+)
(UR2||ECS1Sig)hash
S265
执行ECS2Sig的签名验证
Verify(ECS发布方公共密钥，ECS2Sig，M)
M=内容C1的内容哈希列表集||Kt3哈希值
S266
因ECS2Sig=Sign(ECS签名密钥，M)
且M=内容C1的内容哈希列表集||Kt2哈希值，
故ECS2Sig的验证失败

图 29

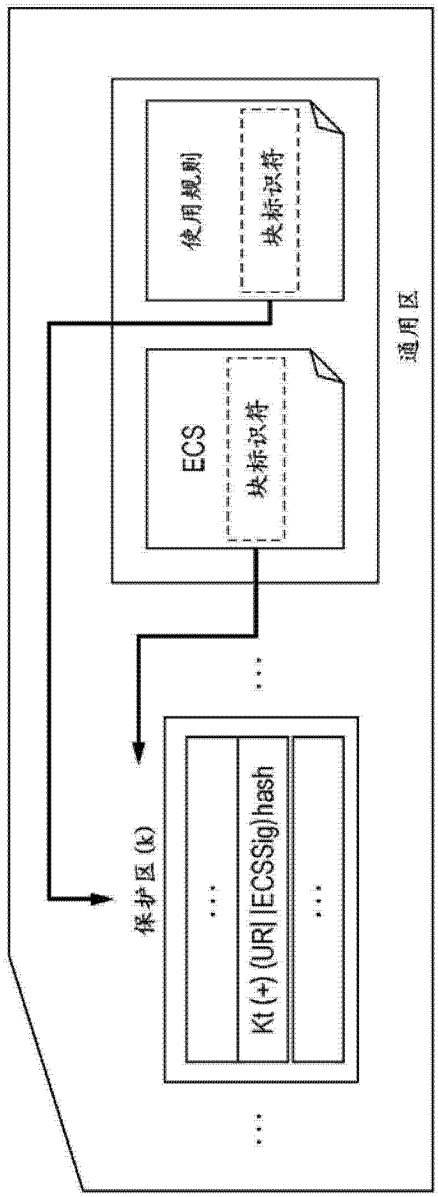

使用规则
块标识符
ECS
块标识符
通用区
保护区(k)
Kt(+)(UR||ECSSig)hash

图 30

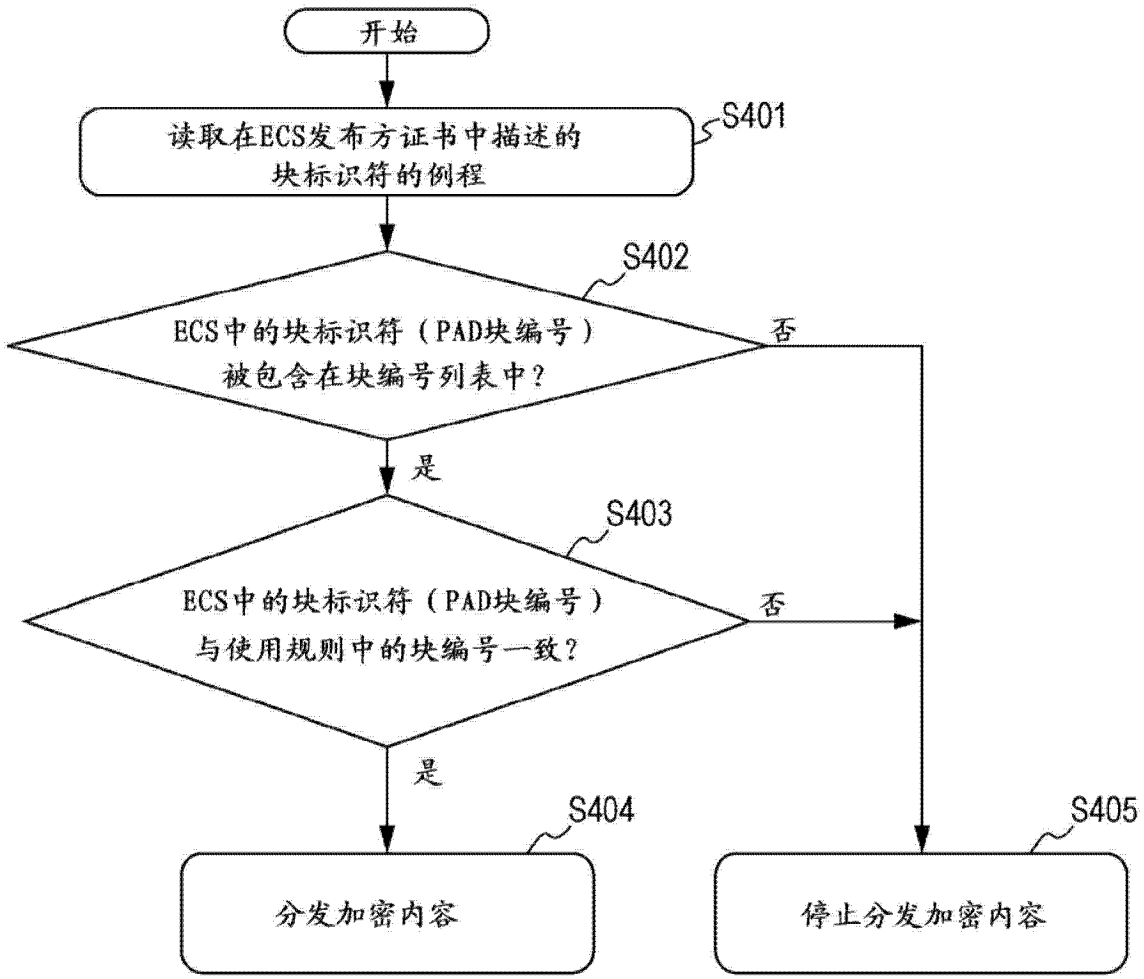

开始
读取在ECS发布方证书中描述的
块标识符的例程
S401
S402
ECS中的块标识符（PAD块编号）
被包含在块编号列表中？
否
是
S403
ECS中的块标识符（PAD块编号）
与使用规则中的块编号一致？
否
是
S404
分发加密内容
S405
停止分发加密内容

图 31

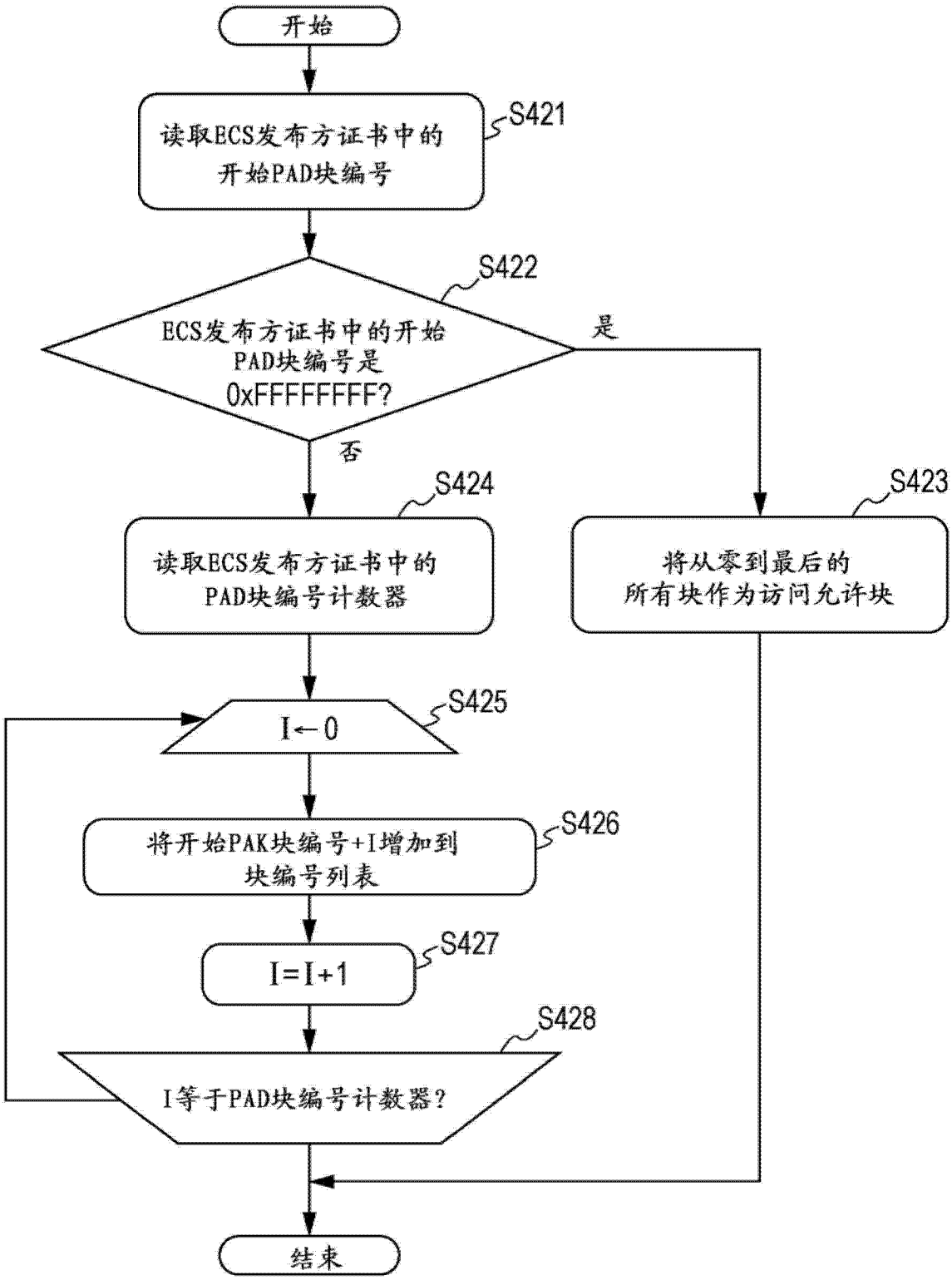

开始
读取ECS发布方证书中的开始PAD块编号
S421
ECS发布方证书中的开始PAD块编号是0xFFFFFFFF?
S422
是
否
读取ECS发布方证书中的PAD块编号计数器
S424
将从零到最后的所有块作为访问允许块
S423
I←0
S425
将开始PAK块编号+I增加到块编号列表
S426
I=I+1
S427
I等于PAD块编号计数器?
S428
结束

图 32

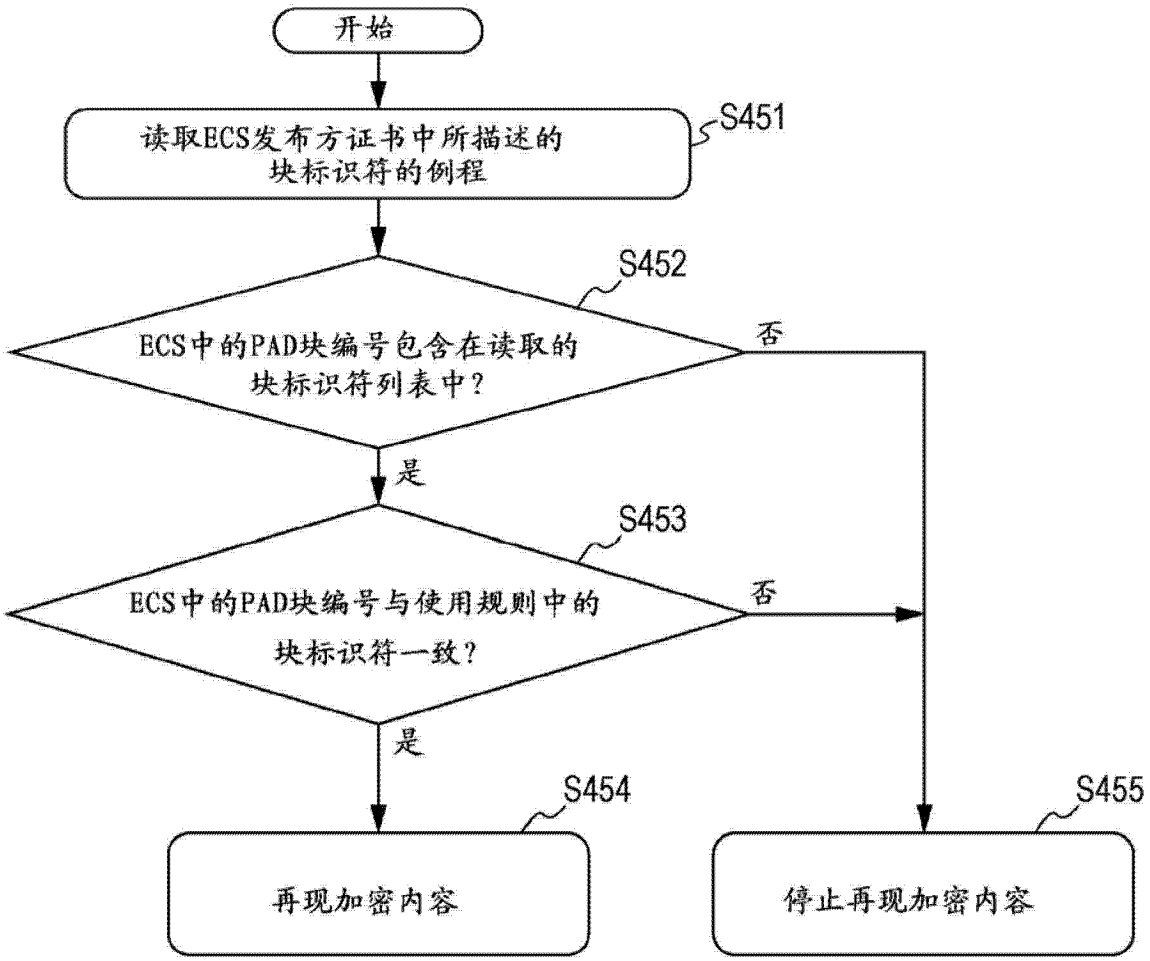

开始
读取ECS发布方证书中所描述的
块标识符的例程
S451
S452
ECS中的PAD块编号包含在读取的
块标识符列表中？
否
是
S453
ECS中的PAD块编号与使用规则中的
块标识符一致？
否
是
S454
再现加密内容
S455
停止再现加密内容

图 33

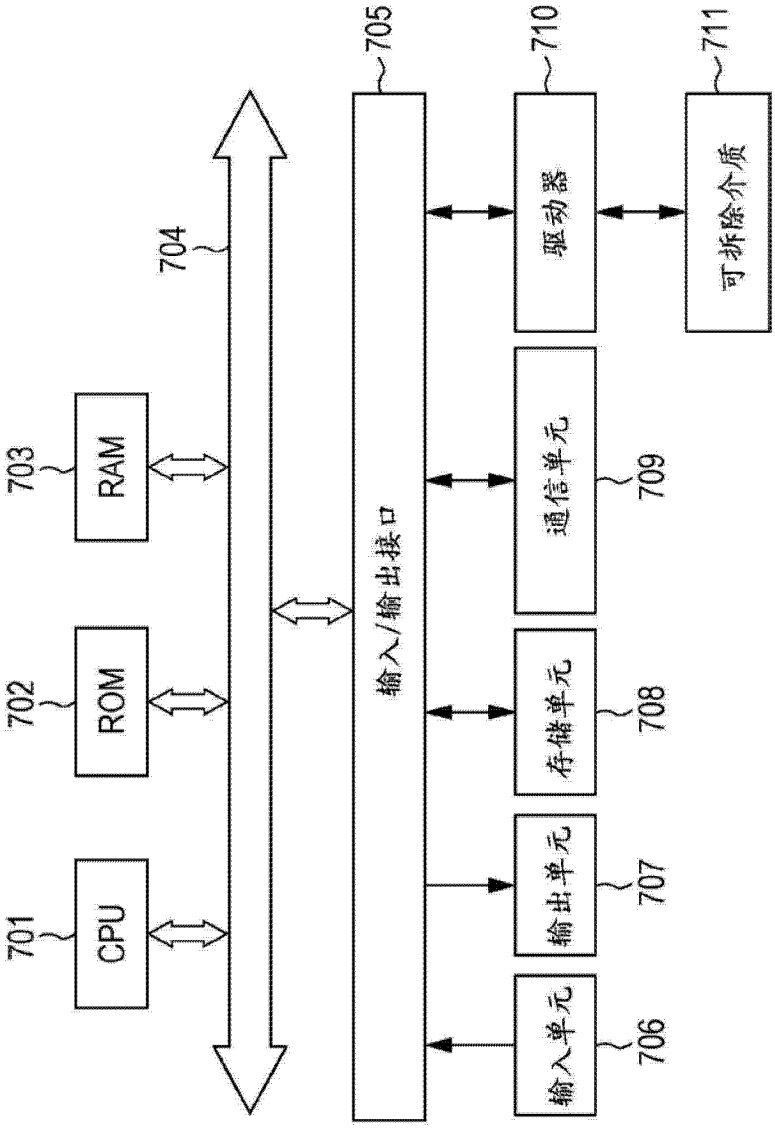

701
CPU
702
ROM
703
RAM
704
705
输入/输出接口
706
输入单元
707
输出单元
708
存储单元
709
通信单元
710
驱动器
711
可拆除介质

图 34

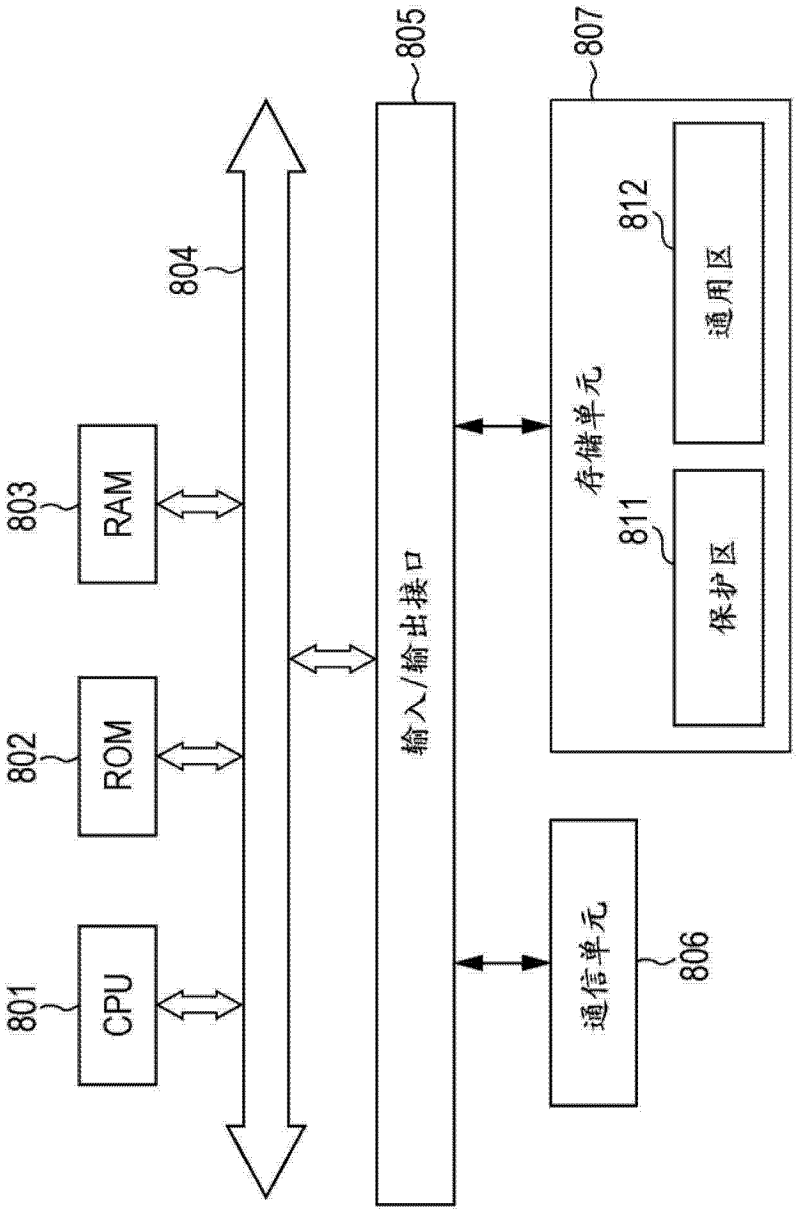

801
CPU
802
ROM
803
RAM
804
805
输入/输出接口
806
通信单元
807
存储单元
811
保护区
812
通用区

图 35