(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 103427984 B
(45)授权公告日 2018.04.06

(21)申请号 201310196937.6

(22)申请日 2013.05.24

(65)同一申请的已公布的文献号
申请公布号 CN 103427984 A

(43)申请公布日 2013.12.04

(30)优先权数据
10-2012-0055527 2012.05.24 KR

(73)专利权人 三星电子株式会社
地址 韩国京畿道

(72)发明人 王卫新 赵熙昌 李元奭 金旼煜 张炯硕

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 钱大勇

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
US 2009164801 A1,2009.06.25,
US 2009282264 A1,2009.11.12,
US 2011215908 A1,2011.09.08,
US 2011246738 A1,2011.10.06,
US 2011252243 A1,2011.10.13,
CN 1490771 A,2004.04.21,
US 2004210707 A1,2004.10.21,
JP 2005165735 A,2005.06.23,
US 2005235143 A1,2005.10.20,
US 2006248346 A1,2006.11.02,
姚荻.一种认证增强的对象存储安全机制设计.《计算机科学》.2010,(第9期),

审查员 肖敬伟

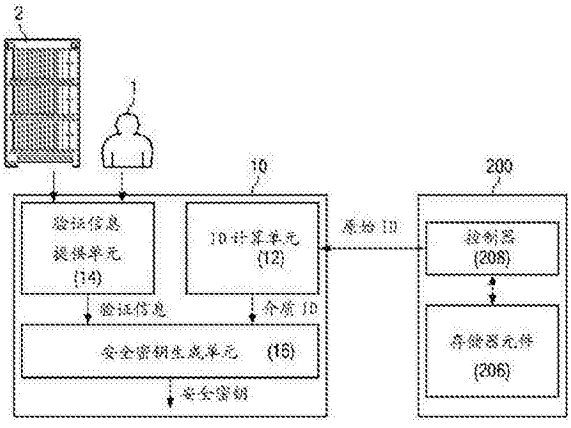
权利要求书3页 说明书15页 附图18页

(54)发明名称

用于使用设备ID和用户验证信息来生成安全密钥的装置

(57)摘要

一种安全密钥生成装置，包括：ID计算单元，其从第一存储设备接收原始ID并从第一原始ID计算第一介质ID(第一存储设备的唯一标识符)；用户验证信息提供单元，其提供用于验证当前用户的用户验证信息；以及安全密钥生成单元，其用于使用第一介质ID和第一用户验证信息两者来生成第一安全密钥。安全密钥用来加密/解密存储在第一存储设备中的内容。安全密钥生成单元使用第二存储设备的第二介质ID生成第一不同的安全密钥，并且使用第二用户的用户验证信息生成第二不同的安全密钥。只有第一安全密钥可以用来解密使用第一安全密钥加密的、存储在第一存储设备中的加密的内容。



CN 103427984 B

1.一种安全密钥生成装置,包括:

ID计算电路,所述ID计算电路被配置为经由存储接口从第一存储设备接收第一原始ID,并且从所述第一原始ID计算第一介质ID,其中所述第一介质ID是所述第一存储设备的数字标识符;

验证信息提供电路,所述验证信息提供电路被配置为向安全密钥生成电路提供用于验证用户的用户验证信息,所述用户验证信息经由输入单元来接收;以及

安全密钥生成电路,所述安全密钥生成电路被配置为使用所述第一介质ID和用户验证信息两者来生成对应的安全密钥,

其中,所述第一原始ID包括通过加密作为被包括在第一存储设备中的第一存储器元件的标识符的第一存储器ID,以及通过加密作为被包括在第一存储设备中的第一控制器的标识符的第一控制器ID而获取的第一加密的存储器ID,以及

其中,所述ID计算电路将第一加密的存储器ID解密为第一存储器ID,从第一存储器ID计算第一存储器导出ID,并且使用第一控制器ID和第一存储器导出ID两者来计算第一介质ID。

2.如权利要求1所述的装置,其中所述第一原始ID是用来计算所述第一介质ID的一个或多个ID数据,并且是与所述第一介质ID不同的数据。

3.如权利要求1所述的装置,其中所述验证信息提供电路从当前用户接收用户验证信息,其中所述安全密钥生成电路被配置为使用第一介质ID和当前用户的用户验证信息两者来生成所述安全密钥。

4.如权利要求2所述的装置,其中:

所述ID计算电路被配置为从第二存储设备接收第二原始ID,并且从所述第二原始ID计算第二介质ID,其中,所述第二介质ID是第二存储设备的数字标识符;

其中所述安全密钥生成电路被配置为生成与所述第二介质ID和用户验证信息两者对应的不同的安全密钥,并且

所述第二原始ID是用来计算所述第二介质ID的一个或多个ID数据,并且是与第二介质ID不同的数据。

5.如权利要求1所述的装置,其中:

所述ID计算电路被配置为从第二存储设备接收第二原始ID,并且从所述第二原始ID计算第二介质ID,其中所述第二介质ID是所述第二存储设备的数字标识符;

其中所述安全密钥生成电路被配置为生成与所述第二介质ID和用户验证信息两者对应的不同的安全密钥,并且

所述第二原始ID是通过加密作为第二存储器元件的标识符的第二存储器ID而获得的第二加密的存储器ID,并且所述ID计算电路将第二加密的存储器ID解密为第二存储器ID,从所述第二存储器ID计算第二存储器导出ID,并且使用所述第二存储器导出ID作为第二介质ID。

6.一种安全密钥生成装置,包括:

存储接口,所述存储接口被配置为从第一存储设备接收第一原始ID并且向处理器提供所述第一原始ID;及

处理器,所述处理器被配置为从第一原始ID计算作为第一存储设备的标识符的第一介

质ID，并且使用所述第一介质ID和用于验证用户的验证信息两者来生成对应的安全密钥，

其中，所述处理器工作在非安全运行模式和安全运行模式之一中，并且验证信息用在将处理器的工作模式从非安全运行模式改变为安全运行模式所需要的验证过程中，

其中，所述处理器包括在非安全运行模式下执行命令的非安全虚拟内核，和在安全运行模式下执行命令的安全虚拟内核，所述非安全虚拟内核检验验证信息并且当成功检验验证信息时生成中断信号，所述处理器响应于所述中断信号将其工作模式从非安全运行模式改变为安全运行模式，并且所述安全虚拟内核生成安全密钥。

7.如权利要求6所述的装置，进一步包括随机存取存储器RAM，其中，RAM包括通过在非安全虚拟内核上执行的命令来存取的第一区域，和可以通过在安全虚拟内核上执行的命令来存取的、并且不与所述第一区域重叠的第二区域，并且在所述非安全虚拟内核上执行的命令不能存取所述第二区域。

8.如权利要求6所述的装置，进一步包括接收验证信息并向所述处理器提供验证信息的输入电路，其中，所述处理器工作在非安全运行模式和安全运行模式之一中，并且在所述安全运行模式下从所述输入电路接收验证信息，并且在所述安全运行模式下生成安全密钥。

9.一种主机设备，包括：

存储接口，所述存储接口被配置为当连接至第一存储设备时从所述第一存储设备接收原始ID，并且向片上系统SoC提供第一原始ID；及

SoC，所述SoC被连接至所述存储接口，

其中所述SoC包括外设逻辑，所述外设逻辑被配置为从所述第一原始ID计算作为所述第一存储设备的唯一标识符的第一介质ID，其中，所述第一原始ID包括第一存储设备的第一存储器ID和被包括在第一存储设备中的控制器的控制器ID；并使用所述第一介质ID和用于验证主机设备的当前用户的用户验证信息两者来生成对应的安全密钥。

10.如权利要求9所述的主机设备，其中所述SoC进一步包括被配置为接收用户验证信息并向所述外设逻辑提供用户验证信息的内核。

11.如权利要求9所述的主机设备，进一步包括由所述SoC控制的输入电路，所述输入电路被配置为从当前用户接收验证信息，并被配置为向所述SoC提供验证信息。

12.如权利要求9所述的主机设备，其中所述SoC进一步包括存储安全密钥的寄存器。

13.如权利要求9所述的主机设备，其中所述外设逻辑被配置为使用安全密钥来加密内容，并且通过所述存储接口向存储设备提供加密的内容。

14.如权利要求9所述的主机设备，其中所述存储接口被配置为从所述第一存储设备接收加密的内容并向所述SoC提供加密的内容，并且所述外设逻辑被配置为从所述第一原始ID计算作为所述第一存储设备的唯一标识符的第一介质ID，并且使用所述第一介质ID和用于验证当前用户的验证信息两者生成用于解密经加密的内容的对应安全密钥。

15.一种存储设备，包括：

存储器元件，所述存储器元件被配置为存储作为第一存储器元件的唯一标识的第一存储器ID，以及通过加密所述第一存储器ID而获取的第一加密的存储器ID；

主机接口，所述主机接口被配置为从主机设备接收用于验证用户的验证信息并向安全密钥生成电路提供验证信息，以及从主机设备接收内容并向加密电路提供内容；

存储器导出ID计算电路，所述存储器导出ID计算电路被配置为从存储器元件中读取加密的存储器ID，通过解密第一加密的存储器ID来获取第一存储器ID，并且使用所述第一存储器ID生成作为所述第一存储器元件的另一个唯一标识符的第一存储器导出ID，以及使用第一存储器导出ID和作为被包括在存储设备中的控制器的标识符的控制器ID来计算第一介质ID；

安全密钥生成电路，所述安全密钥生成电路被配置为使用验证信息和第一介质ID两者来生成安全密钥；以及

加密电路，所述加密电路被配置为使用安全密钥来加密内容，并且在所述存储器元件中存储加密的内容。

16.如权利要求15所述的存储设备，其中由所述主机设备提供验证信息来作为安全数字SD卡标准命令的参数。

17.如权利要求15所述的存储设备，进一步包括随机数发生器，其中所述安全密钥生成电路被配置为通过进一步使用由随机数发生器生成的随机数来生成安全密钥。

18.如权利要求17所述的存储设备，其中所述存储设备根据信赖的计算组的opal安全子系统类OPAL SSC规范来工作。

19.一种安全密钥生成方法，包括：

将第一存储设备电连接至安全密钥生成装置；

在所述安全密钥生成装置处从所述第一存储设备接收第一原始ID，并通过使用所述安全密钥生成装置从所述第一原始ID计算作为所述第一存储设备的唯一标识符的第一介质ID；

在所述安全密钥生成装置处直接从当前用户接收用于验证当前用户的用户验证信息，或者从通过网络连接的另一设备接收用户验证信息；以及

在所述安全密钥生成装置中利用所述第一介质ID和所述用户验证信息两者来生成安全密钥，

其中，所述第一原始ID包括通过加密作为被包括在第一存储设备中的第一存储器元件的标识符的第一存储器ID，以及通过加密作为被包括在第一存储设备中的第一控制器的标识符的第一控制器ID而获取的第一加密的存储器ID，以及

其中，所述方法进一步包括将第一加密的存储器ID解密为第一存储器ID，从第一存储器ID计算第一存储器导出ID，并且使用第一控制器ID和第一存储器导出ID两者来计算第一介质ID。

用于使用设备ID和用户验证信息来生成安全密钥的装置

[0001] 对相关申请的交叉引用

[0002] 本申请要求于2012年5月24日在韩国知识产权局提交的韩国专利申请No.10-2012-0055527的优先权，通过引用将其内容全面合并于此。

技术领域

[0003] 本发明构思涉及一种安全密钥生成装置，并且更具体地，涉及一种使用设备ID和用户验证信息(诸如用户密码)两者来生成属于特定设备和特定用户的安全密钥的装置、使用安全密钥的存储设备、和安全密钥生成方法。

背景技术

[0004] 近来，各种类型的便携式存储设备被引入市场。这些便携式存储设备在存储容量上变得更大而在体积上变得更小，并且它们的接口可以插入通常可用的主机设备(例如，计算机、按需打印机、蜂窝电话、数字电视等)/从其移除。从而，对于便携式存储设备的需求正在增加。便携式存储设备的一些例子包括使用闪存作为存储介质的存储卡(例如，SD卡)、可以连接至通用串行总线(USB)端口的USB存储器(“USB驱动器”)和固态存储器(SSD)。另外，便携式硬盘已被评价为便宜的存储设备，并且引入了外部硬盘。外部硬盘驱动器提供了不同于固定到个人计算机的传统硬盘驱动器的便携性。

[0005] 这种趋势不限于便携式存储设备。可以连接至便携式存储设备的主机设备也变得更小。因此，创建了其中可以以任何时间任何地点享用存储在便携式存储设备中的数字内容的环境。随着此环境的创建，越来越多地用数字数据的形式分发和出售商业化产生的数字内容。这提高了防止数字内容被非法复制的技术的重要性。

[0006] 为了防止数字内容的非法复制，数字内容可以被加密然后存储在便携式存储设备中。这里，使用特定的数字加密密钥对数字内容加密。当使用特定设备时，使用仅与特定设备关联的数字加密密钥的加密和解密技术移除对于数据的保护。

发明内容

[0007] 本发明的方面提供了一种用于生成属于特定设备和特定用户两者的安全密钥的装置、使用安全密钥加密内容并存储加密的内容的存储设备、以及安全密钥生成方法。传统的加密和解密技术使用仅与特定的设备关联的密钥，并且当使用特定设备时移除对于数据的保护，而本发明的方面提供了一种用于生成属于特定设备和特定用户两者的安全密钥的装置，使得仅特定的人可以(例如，在特定的设备上)播放内容，以便保护他的或她的隐私。本发明的方面提供了一种生成并利用不但属于特定设备而且属于特定用户的安全密钥的技术。

[0008] 本发明的方面还提供了一种用于使用特定设备的标识符和由用户输入的用户验证信息两者来生成安全密钥的装置、使用安全密钥加密内容并存储加密的内容的存储设备、以及安全密钥生成方法。

[0009] 本发明的方面还提供了一种用于在支持信赖的计算的主机设备中安全地生成安全密钥的装置。

[0010] 本发明的方面还提供了一种在信赖的运行环境中生成安全密钥的主机设备，以便防止设备ID、用户验证信息、和生成的安全密钥的泄漏。

[0011] 然而，本发明的方面不限于在此阐述的一个。通过引用下面给出的本发明的详细描述，本发明的以上和其它方面对于本发明属于的领域的一名普通技术人员将变得更加清楚。

[0012] 根据本发明的一方面，提供了一种安全密钥生成装置，包括：ID计算单元，其从存储设备接收原始ID，并且从原始ID计算作为存储设备的唯一标识符的介质ID；验证信息提供单元，其向安全密钥生成单元提供用于验证用户的验证信息；及安全密钥生成单元，其使用介质ID和验证信息两者来生成安全密钥。

[0013] 根据本发明的另一方面，提供了一种安全密钥生成装置，包括：存储接口，其从存储设备接收原始ID并且向处理器提供原始ID；及处理器，其从原始ID计算作为存储设备的唯一标识符的介质ID，并且使用介质ID和用于验证用户的验证信息两者来生成安全密钥。

[0014] 根据本发明的另一方面，提供了一种存储设备，包括：存储器元件，其存储作为存储器元件的唯一标识符的存储器ID，以及通过加密存储器ID而获得的加密的存储器ID；主机接口，其从主机接收用于验证用户的验证信息并向安全密钥生成单元提供验证信息，并且从主机设备接收内容并且向加密单元提供内容；存储器导出ID计算单元，其从存储器元件读取加密的存储器ID，通过解密经加密的存储器ID而获得存储器ID，以及使用存储器ID生成作为存储器元件的另一个唯一标识符的存储器导出ID；加密密钥生成单元，其使用验证信息和存储器导出ID两者来生成安全密钥；以及加密单元，其使用安全密钥来加密内容，并且在存储器单元中存储加密的内容。

[0015] 一种安全密钥生成方法，包括：将存储设备电连接至安全密钥生成装置；从存储设备接收原始ID，以及通过使用安全密钥生成装置从原始ID中计算作为存储设备的唯一标识符的介质ID；通过使用安全密钥生成装置从用户直接接收用于验证用户的验证信息，或者从通过网络连接的另一设备接收验证信息；以及通过使用安全密钥生成装置，利用介质ID和验证信息两者来生成安全密钥。

[0016] 现在将参照附图在下文中更加充分地描述本发明，附图中示出本发明的示范性实施例。然而，可以在不同的形式中实现此发明，而不应该认为此发明限于此处阐述的示范性实施例。相反地，提供示范性实施例以使得本公开是彻底和完整的，并且对本领域技术人员充分地表达本发明的范围。在整个说明书中，相同的参考标号指示相同的组件。在附图中，为了清楚，放大了层和区域的厚度。在描述本发明的上下文(尤其是在下面权利要求的上下文)中术语“一”和“一个”和“该”及类似对象的使用被认为是涵盖了单数和复数两者，除非在此指示除外或者同上下文明显矛盾。除非另作说明，否则术语“包括”、“具有”、“包含”和“含有”被认为是开放性的术语(即，意思是“包括，但不限于”)。

[0017] 除非另外定义，否则这里使用的全部技术和科学术语具有此发明所属的领域的一位普通技术人员所通常理解的一样的意思。注意到，除非另作说明，否则任何和所有例子的使用或者在此提供的示范性术语旨在仅仅更好地阐明发明，而不是对于发明的范围的限制。此外，除非另作定义，否则所有在通用词典中定义的术语可能不过度解释。

附图说明

[0018] 参照附图，通过详细描述本发明的示范性实施例，本发明的以上及其它方面和特征将变得更加清楚，其中：

[0019] 图1是根据本发明的示范性实施例的安全密钥生成装置的框图；

[0020] 图2和3是示出关于包括在图1的安全密钥生成装置中的ID计算单元的配置的框图；

[0021] 图4是示出包括在图1的安全密钥生成装置中的ID计算单元的操作的参考图；

[0022] 图5是根据本发明的示范性实施例的安全密钥生成装置的框图；

[0023] 图6和7是当安全密钥生成装置是支持信赖的计算的装置时，图5的安全密钥生成装置的框图；

[0024] 图8是根据本发明的示范性实施例的安全密钥生成装置的框图；

[0025] 图9是示出在图8的安全密钥生成装置中的外设逻辑的位置的参考图；

[0026] 图10和11是当安全密钥生成装置执行加密和解密时，图8的安全密钥生成装置的框图；

[0027] 图12和13是根据本发明的示范性实施例的存储设备的框图；

[0028] 图14是根据本发明的示范性实施例的存储系统的框图；

[0029] 图15是示出根据本发明的示范性实施例的安全密钥生成方法的流程图；

[0030] 图16是示出根据本发明的示范性实施例的生成安全密钥并使用安全密钥加密内容的方法的流程图；

[0031] 图17至20是示出根据本发明的示范性实施例的生成介质ID的方法的流程图；

[0032] 图21是示出根据本发明的示范性实施例的生成安全密钥并使用安全密钥解密内容的方法的流程图；

[0033] 图22是示出根据本发明的示范性实施例的不能解密非法复制的内容的过程的流程图；以及

[0034] 图23是示出根据本发明的示范性实施例的，当输入不正确的用户验证信息时不能解密内容的过程的流程图。

具体实施方式

[0035] 现在将参照图1描述根据本发明的示范性实施例的安全密钥生成装置10的配置和操作。根据当前示范性实施例的安全密钥生成装置10连接至非易失性存储设备200，并且使用介质ID和用于验证用户1的验证信息来生成安全密钥。介质ID是存储设备200的唯一标识符(unique identifier)。

[0036] 安全密钥生成装置10连接至存储设备200并且从存储设备200接收原始ID。原始ID是用于计算介质ID的一个或多个ID数据。原始ID是不同于介质ID的数据。安全密钥生成装置10从原始ID而不是从用于验证用户1的验证信息来生成介质ID。从而，从存储设备200中，安全密钥生成装置10不接收介质ID而接收用于生成介质ID的原始ID(源数据)。这可以防止介质ID的泄漏或检测。安全密钥生成装置10可以存储用于从原始ID生成介质ID的数据。

[0037] 根据当前示范性实施例的安全密钥生成装置10包括ID计算单元12、验证信息提供

单元14、和安全密钥生成单元16。ID计算单元12接收存储在存储设备中的原始ID，并且从原始ID计算介质ID(其为存储设备的唯一标识符)。

[0038] 验证信息提供单元14向安全密钥生成单元16提供用于验证用户1的验证信息。可以通过用户1直接将验证信息输入到安全密钥生成装置10。可替换地，用户验证服务器2可以向安全密钥生成装置10提供用户验证信息。从而，验证信息提供单元14可以向安全密钥生成单元16提供从用户1或从用户验证服务器2接收的验证信息。例如，验证信息可以是用在特定会员服务中的用户验证信息、用户标识信息、或个人信息。个人信息是关于个人的个人资料的信息。个人信息的例子可以包括地址、生日、电话号码、邮箱地址、居民注册号、用户的生物测定信息、及与用户1使用的金融安全卡上的特定号码对应的代码。

[0039] 安全密钥生成单元16使用介质ID和验证信息来生成安全密钥。在生成安全密钥中使用介质ID意味着介质ID被输入至少一次以生成安全密钥。此外，在生成安全密钥中使用验证信息意味着验证信息被输入至少一次以生成安全密钥。

[0040] 安全密钥生成单元16可以通过对于介质ID和验证信息执行二元运算来生成安全密钥。二元运算的例子可以包括和(AND)、或(OR)、或非(NOR)、异或(XOR)和与非(NAND)运算。安全密钥生成单元16还可以通过对介质ID和验证信息执行串连接(STRCAT)运算来生成安全密钥。在STRCAT运算中，可以不按固定的次序来连接串。从而，可以按此次序或相反的次序来连接介质ID和验证信息。

[0041] 安全密钥生成单元16可以仅使用介质ID和验证信息，或除了介质ID和验证信息之外使用一个或多个可变或不可变的数据来生成安全密钥。

[0042] 仅当用户验证信息、介质ID、和安全密钥计算公式都可用时才生成安全密钥。因此，只要安全密钥自身不被泄漏，即使安全密钥计算公式被暴露，除非用户验证信息和介质ID两者都被识别，否则也不能生成安全密钥。介质ID是不被泄漏并且仅可以从在存储设备200提供的原始ID上的运算获取的值。此外，验证信息是不容易泄漏的值，因为它将由用户1管理以防止它的泄漏。因此，根据当前示范性实施例的安全密钥生成装置10生成属于存储设备200也属于用户1的安全密钥。

[0043] 现在将参照图2和3更加详细地描述从原始ID计算介质ID的ID计算单元12的操作。

[0044] 如上所述，原始ID是与介质ID不同的数据，并且也用来标识存储设备200的至少第一部分。例如，存储设备200可以包括第一部分和第二部分，并且向ID计算单元12提供作为第一部分的标识符的第一原始ID和作为第二部分的标识符的第二原始ID。这里，原始ID包括第一原始ID和第二原始ID。

[0045] 参照图2，ID计算单元12从存储设备200接收加密的存储器ID 264，以作为原始ID的一个分量。加密的存储器ID 264是通过加密作为包括在存储设备200中的存储器元件206的唯一标识符的存储器ID 262而获得的数据。存储器ID 262可以是当制造存储器元件206时由存储器元件206的厂商编程的数据。存储器ID 262可以被存储在不按与存储在用户区域的数据的相同的方式存取的系统区域中。如果存储器ID 262被存储在用户区域中，则其可以被删除、修改、和泄漏。如果存储器ID 262存储在不能存取的系统区域中，则其不能被删除、修改或泄漏。

[0046] 参照图3，ID计算单元12从存储设备200接收控制器验证信息，作为原始ID的另一分量。安全密钥生成装置10和包括在存储设备200中的控制器208可以彼此相互验证。控制

器验证信息是控制器208向安全密钥生成装置10提供用于该相互验证的数据。

[0047] 图4是示出ID计算单元12生成介质ID的过程的参考图。

[0048] ID计算单元12通过解密经加密的存储器ID 264来获取存储器ID 262，并从存储器ID 262中生成存储器导出ID。此外，ID计算单元12从控制器验证信息中获得作为存储器控制器208的唯一标识符的控制器ID。

[0049] 可以以加密的形式从存储设备200接收用于解密经加密的存储器ID 264的第一解密密钥。此外，可以在包括在安全密钥生成装置10中的存储单元(未示出)中存储用于解密经加密的第一解密密钥的第二解密密钥。

[0050] 从而，ID计算单元12可以从存储设备200接收加密的第一解密密钥，并且通过使用第二解密密钥解密经加密的第一解密密钥来获得第一解密密钥。然后，ID计算单元12可以使用第一解密密钥来将加密的存储器ID 264解密成存储器ID 262。

[0051] 存储器导出ID是存储器元件206的另一唯一标识符。从而，存储器元件206可以具有两个唯一标识符，即，作为由存储器元件206的厂商编程的唯一标识符的存储器ID 262，和使用存储器ID 262生成的存储器导出ID。存储器ID 262存储在存储器元件206中。另一方面，存储器导出ID是不存储在存储器元件206中，而是由连接至存储设备200的安全密钥生成装置10生成的值。

[0052] ID计算单元12可以使用控制器验证信息来生成控制器ID。控制器验证信息可以包括控制器验证证书ID和控制器208的唯一标识代码。ID计算单元12可以使用控制器验证证书ID和唯一标识符代码来生成控制器ID。例如，ID计算单元12可以通过在控制器验证证书ID和唯一标识符代码上执行串连接操作来生成控制器ID。

[0053] ID计算单元12可以使用存储器导出ID和控制器ID来生成介质ID。例如，ID计算单元12可以通过将存储器导出ID和控制器ID输入到二元运算或串连接运算中来生成介质ID。

[0054] 现在将参照图5至7来描述根据本发明的示范性实施例的安全密钥生成装置20的配置和操作。

[0055] 参照图5，根据当前示范性实施例的安全密钥生成装置20可以包括处理器102和存储接口104。安全密钥生成装置20可以进一步包括用作处理器102的系统存储器并且临时存储由处理器102运行的命令的随机存取存储器(RAM)106，和接收用户验证信息的输入单元108。处理器102、存储接口104、RAM 106、和输入单元108可以连接至内部系统总线110。

[0056] 如图5中所示，存储接口104可以中继在安全密钥生成装置20和存储设备200之间交换的数据。存储接口104可以从存储设备200接收原始ID，并且通过系统总线110向处理器102提供所接收的原始ID。

[0057] 处理器102从所接收的原始ID中计算介质ID(存储设备200的唯一标识符)。处理器102可以使用介质ID和用于验证用户的验证信息两者来生成安全密钥。输入单元108可以从用户接收验证信息，并且向处理器102提供所接收的验证信息。处理器102可以使用安全密钥以用于各种用途。例如，处理器102可以使用安全密钥作为高安全级别的用户验证信息，或者作为用于要存储在存储设备200中的内容的加密密钥。

[0058] 根据当前示范性实施例的安全密钥生成装置20可以支持安全运行环境。安全运行环境是保证通过诸如处理器和操作系统的组件而安全运行程序的环境。可以通过完整性和机密性来保证安全运行。通常，已知基于硬件的安全运行环境方法比基于软件的安全运行

环境方法更安全。假设根据当前示范性实施例的安全密钥生成装置20提供基于硬件的安全运行环境。

[0059] 参照图6和7，安全密钥生成装置20可以包括处理器102，处理器102包括双核以便划分处理运行环境。处理器102可以包括两个或更多个物理分离的内核，并且使用它们分别用于安全运行模式和非安全运行模式。可替换地，处理器102可以事实上将一个内核拆分成虚拟内核，并且使用它们分别用于安全运行模式和非安全运行模式。在图6和7中，将描述在其中处理器102包括两个虚拟内核120和124的例子。

[0060] 安全密钥生成装置20可以禁止在不提供安全运行环境的非安全运行模式下运行的过程存取通过在提供安全运行环境的安全运行模式下运行的过程所生成的数据。从而，在安全运行模式下存取的数据可以与在非安全模式下存取的数据分离。例如，RAM 106可以包括：可以通过在非安全虚拟内核120上运行的命令存取的第一区域，和仅可以通过在安全虚拟内核124上运行的命令存取的、并且不与第一区域重叠的第二区域。

[0061] 如果处理器102的内核被逻辑地分成用于在安全运行模式下的处理运行的安全虚拟内核124和用于在非安全运行模式下的处理运行的非安全虚拟内核120，并且相应地工作，则可以通过上下文的切换机制进行安全运行模式和非安全运行模式之间的每次变化。

[0062] 作为可以被包括以提供上述安全运行环境的相关技术，处理器102可以采用ARM的TRUSTZONE、英特尔的无线TPM、德州仪器的M-Shield和飞思卡尔的安全技术、SafeNet的SafeXcel TPM、SafeNet的SafeZone、Discretix的安全平台、以及高通的SecureMSM的至少一个。

[0063] 对于要在处理器102的安全运行模式下运行的过程，可能需要验证程序。验证程序可以是接收用户验证信息并检验所接收的验证信息是否与预存储的验证信息相同的程序。如果检验出所接收的验证信息与预存储的验证信息相同，则可以生成用于将处理器102的工作模式从非安全运行模式改变为安全运行模式的中断信号。然后，处理器102响应于中断信号可以切换至安全运行模式。参照图6，工作在非安全模式下的处理器102执行用户验证以便切换至安全运行模式。对于用户验证，处理器102从输入单元108接收用户验证信息。当使用用户验证信息成功地验证用户时，处理器102经由监视过程122改变虚拟内核(例如，从非安全虚拟内核120切换为安全虚拟内核124)。

[0064] 从而，当处于非安全运行模式中时，根据当前示范性实施例的安全密钥生成装置20的处理器102接收用户验证信息，以用于改变它的运行模式。结果，处理器102将它的运行模式改变为安全运行模式，并且在安全运行模式下生成安全密钥。因为根据当前示范性实施例的安全密钥生成装置20在安全运行模式下生成安全密钥，所以可以防止用户验证信息、原始ID、存储器ID、介质ID等等的泄漏。

[0065] 根据当前示范性实施例的安全密钥生成装置20的处理器102还可以在改变为安全运行模式之后接收用户验证信息和原始ID，并且在安全运行模式下生成安全密钥。参照图7，根据当前示范性实施例的安全密钥生成装置20在改变为安全运行模式之后接收用户验证信息和原始ID，并且从其生成安全密钥。包括在根据当前示范性实施例的安全密钥生成装置20中的RAM106可以包括仅当处理器102工作在安全运行模式下时才能被存取的安全区域，并且处理器102可以在安全区域中存储验证信息、原始ID、介质ID和安全密钥。

[0066] 根据当前示范性实施例，当安全密钥生成装置20接收用户验证信息时，其已经工

作在安全运行模式下。从而，可以防止用户验证信息、原始ID、存储器ID、介质ID等等的泄漏。

[0067] 现在将参照图8至11来描述根据本发明的另一示范性实施例的安全密钥生成装置30的配置和操作。

[0068] 图8示出根据本发明的示范性实施例的安全密钥生成装置30的配置。参照图8，根据当前示范性实施例的安全密钥生成装置30包括片上系统(SoC)302和连接至SoC 302的存储接口104。根据当前示范性实施例的存储接口104当连接至存储设备200时从存储设备200接收原始ID，并且向SoC 302提供所接收的原始ID。

[0069] SoC 302是作为单个芯片的具有各种功能的系统的实现。根据当前示范性实施例的SoC 302包括外设逻辑320，外设逻辑320从原始ID计算介质ID(即，存储设备200的唯一标识符)，并使用介质ID和用于验证用户的验证信息两者来生成安全密钥。

[0070] SoC 302可以进一步包括执行命令的内核322(处理器)。内核322可以读取存储在包括在安全密钥生成装置30中的RAM(未示出)中的命令，并且执行所读取的命令(例如，用于从存储设备200读取原始ID的读取命令)。可以在SoC 302内部或外部提供RAM。内核322控制安全密钥生成装置30的输入/输出相关操作。例如，内核322通过输入单元108从用户接收用户验证信息输入。内核322向外设逻辑320提供用户验证信息。

[0071] 外设逻辑320从内核322接收用户验证信息，但是也可以在不使用内核322的情况下直接从存储接口104接收原始ID。为此，参照图9，外设逻辑320可以连接至存储接口104和内核322之间的数据通路325。外设逻辑320可以通过数据通路325从存储设备200接收原始ID，而不用向内核322发送原始ID。因为内核322可能会受到黑客攻击，并且因此不使用原始ID执行操作，外设逻辑不向内核322发送原始ID。

[0072] 因此，在安全密钥的生成中，外设逻辑320独立于内核322工作。外设逻辑320负责除了从内核322接收用户验证信息的、与安全密钥的生成有关的所有操作。此外，外设逻辑320不运行存储在RAM中的程序。而是，外设逻辑320仅执行存储在包括在外设逻辑320中的非易失性存储器(诸如，只读存储器(ROM))中的安全密钥生成程序。

[0073] 外设逻辑320可以在包括在SoC 302中的寄存器324中存储所生成的安全密钥。

[0074] 意欲偷取安全密钥、介质ID、存储器ID等等的黑客程序通常在内核322上运行。因此，因为独立于内核322的外设逻辑320负责与安全密钥的生成有关的所有操作，所以根据当前示范性实施例的安全密钥生成装置30可以有效地防止与安全密钥的生成有关的数据的泄漏(例如，被盗)。

[0075] 参照图10，根据当前示范性实施例的安全密钥生成装置30可以使用安全密钥来加密内容，并且在连接至安全密钥生成装置30并且被提供有生成用来生成安全密钥的介质ID的原始ID的存储设备200中存储加密的内容。为了增加安全性，外设逻辑320还可以负责要在存储设备200中存储的内容的加密。外设逻辑320还可以负责要从存储设备200检索的加密的内容的解密。为此，外设逻辑320可以包括加密/解密引擎321。加密/解密引擎321可以使用存储在寄存器324中的安全密钥来作为加密/解密密钥。内核322可以通过输入单元108从用户接收用户验证信息输入，也可以通过读取内部存储装置304来获得用户验证信息。

[0076] 参照图11，连接至存储设备200的安全密钥生成装置30可以解密存储在存储设备200中的加密的内容。为了解密经加密的内容，安全密钥生成装置30应该生成存储设备200

的加密的内容的解密密钥。具体地，安全密钥生成装置30可以从存储设备200接收原始ID，从安全密钥生成装置30的用户接收验证信息，从原始ID生成存储设备200的介质ID，然后使用介质ID和验证信息生成加密的内容的解密密钥。内核322可以通过输入单元108从用户接收用户验证信息输入，也可以通过读取内部存储装置304来获得用户验证信息。

[0077] 上述安全密钥生成装置10、20和30的每个可以应用于计算机、超移动PC(UMPC)、工作站、网络书籍、个人数字助理(PDA)、便携式计算机、网络平板、无线电话、移动电话、智能电话、电子书、便携式多媒体播放器(PMP)、便携式游戏设备、导航设备、黑匣子、数码相机、三维电视、数字录音器、数字音频播放器、数字照相机、数字图像播放器、数字摄像机、数字视频播放器、能够在无线环境中发送/接收信息的设备、构成家庭网络的各种电子设备之一、构成计算机网络的各种电子设备之一、构成电信通信网络的各种电子设备之一、射频识别(RFID)设备、或者构成计算机系统的各种组件之一。

[0078] 现在将参照图12至14来描述根据本发明的示范性实施例的存储设备40。根据当前示范性实施例的存储设备40具有加密功能。从而，当存储设备40连接至主机设备并且从主机设备接收要存储的数据时，其没有将所接收的数据原样存储，而是加密所接收的数据，然后存储加密的数据。

[0079] 根据当前示范性实施例的存储设备40通过使用从主机设备接收的用户验证信息和包括在存储设备40中的存储器元件206的存储器导出ID，来生成用于加密所接收的数据的加密密钥。

[0080] 现在将参照图12描述根据当前示范性实施例的存储设备40的配置和操作。参照图12，根据当前示范性实施的存储设备40可以包括存储器元件206、主机接口210、存储器导出ID计算单元212、安全密钥生成单元214、和加密单元216。

[0081] 主机接口210从主机设备接收用于验证用户的验证信息，并且向安全密钥生成单元214提供验证信息。此外，主机接口210从主机设备接收内容(例如，数据)并且向加密单元216提供内容。

[0082] 存储器元件206存储存储器ID 262和通过加密存储器ID 262而获得的加密的存储器ID 264。可以将存储器元件206的存储区域划分成用户区域和系统区域。不能用与存取用户区域的相同方式存取系统区域。优选地在系统区域中存储存储器ID 262和加密的存储器ID 264。

[0083] 存储器元件206可以是非易失性存储器，并且可以是使用NAND(与非)闪存、NOR(或非)闪存、相变随机存取存储器(PRAM)、磁性随机存取存储器(MRAM)、或电阻随机存取存储器(RRAM)作为存储介质的芯片或封装。存储器元件206可以安装在诸如层叠封装(Package on Package,PoP)、球栅阵列(Ball grid array,BGA)、芯片尺寸封装(Chip scale packafe,CSP)、塑料带引线芯片载体(Plastic Leaded Chip Carrier,PLCC)、塑料双列直插封装(Plastic Dual In-Line Package,PDIP)、叠片内裸片封装(Die in Waffle Pack)、晶片内裸片形式(Die in Wafer Form)、板上芯片(Chip On Board,COB)、陶瓷双列直插封装(Ceramic Dual In-Line Package,CERDIP)、塑料标准四边扁平封装(Plastic Metric Quad Flat Pack,MQFP)、薄型四边扁平封装(Thin Quad Flat-Pack,TQFP)、小外型集成电路(Small Outline Integrated Circuit,SOIC)、缩小型小外型封装(Shrink Small Outline Package,SSOP)、薄型小外型封装(Thin Small Outline Package,TSOP)、薄型四

边扁平封装(Thin Quad Flat-Pack,TQFP)、系统级封装(System In Package,SIP)、多芯片封装(Multi Chip Package,MCP)、晶片级结构封装(Wafer-level Fabricated Package,WFP)、晶片级处理堆叠封装(Wafer-Level Processed Stack Package,WSP)的封装上。

[0084] 存储器导出ID计算单元212从存储器元件206读取加密的存储器ID264,通过解密经加密的存储器ID 264而获得存储器ID 262,并且使用存储器ID 262生成作为存储器元件206的另一个唯一标识符的存储器导出ID。

[0085] 安全密钥生成单元214使用验证信息和存储器导出ID两者来生成安全密钥。安全密钥生成单元214用与图1-4的安全密钥生成装置10的安全密钥生成单元16相同的方式生成安全密钥。

[0086] 加密单元216使用安全密钥加密内容(数据),并且在存储器单元206中存储加密的内容。

[0087] 当加密从主机设备接收的内容并存储加密的内容时,根据当前示范性实施例的存储设备40使用通过反映包括在存储设备40中的存储器元件206的唯一标识符而生成的加密密钥。因此,即使非法复制存储在存储设备40中的加密的内容,也能防止其被解密。这是因为存储非法复制的加密内容的存储设备不具有与存储原始加密内容的存储设备40中的介质ID相同的介质ID。

[0088] 通过进一步反映用于验证用户的用户验证信息来生成在根据当前示范性实施例的存储设备40中生成的加密密钥。因此,当用户验证信息不可用时,不能解密存储在存储设备40中的内容。

[0089] 根据当前示范性实施例的存储设备40可以用作包括在云计算服务的云服务器中的存储设备。从而,使用用户的验证信息和存储设备40的介质ID两者来加密由云计算服务的用户所上传的内容或数据,然后进行相应地存储。在这种情况下,除非被泄漏的内容或数据被存储在存储设备40(其为最初存储被泄漏的内容或数据的存储设备)中,以及除非用户的验证信息可用,否则即使在服务器端被黑客攻击并泄漏(例如,盗取)加密的内容或数据,它们也不能被解密。因此,当根据当前示范性实施例的存储设备40被包括在云计算服务的云服务器中,并用作所上传的内容或数据的存储介质时,可以减小由用户上传的内容或数据将来被泄漏的概率。

[0090] 根据当前示范性实施例的存储设备40可以满足安全数字(SD)协会的SD卡标准。在这种情况下,主机接口210可以向安全密钥生成单元214提供所接收的验证信息作为根据SD卡标准的命令的参数。

[0091] 根据当前示范性实施例的存储设备40可以遵照固态存储器(SSD)或硬盘驱动器(HDD)(在其中包括闪存)标准。在这种情况下,主机接口210可以是支持用于大量存储设备的通信命令的物理接口,例如高级技术附件(ATA)、串行ATA(SATA)、小型计算机小型接口(SCSI)、PCI-Express(PCI-E)或通用串行总线(USB)。

[0092] 参照图13,根据当前示范性实施例的存储设备40可以通过另外使用随机数来生成安全密钥。从而,安全密钥生成单元214可以使用随机数、验证信息、和介质ID的所有来生成安全密钥。根据当前示范性实施例的存储设备40可以进一步包括随机数发生器217,其生成随机数并向安全密钥生成单元214提供所生成的随机数。根据当前示范性实施例的存储设备40可以根据可信计算组的opal安全子系统类(OPAL SSC)规范来工作。

[0093] 现在将参照图14来描述根据本发明的示范性实施例的存储系统1000。

[0094] 参照图14，存储系统1000包括非易失性存储器件1100和控制器1200。以上针对图1、2和3描述的存储设备200可以被配置为用于实现图14的存储系统1000(1100和1200)。

[0095] 非易失性存储器件1100可以包括一个或多个如上所述的存储器元件206。

[0096] 控制器1200连接至主机设备和非易失性存储器件1100。控制器1200被配置为响应于来自主机设备的请求而存取非易失性存储器件1100。例如，控制器1200可以被配置为控制非易失性存储器件1100的读/写/擦除/后台操作。控制器1200可以被配置为提供在非易失性存储器件1100和主机设备之间的接口。控制器1200可以被配置为驱动用于控制非易失性存储器件1100的固件。

[0097] 控制器1200进一步包括诸如RAM、处理单元、主机接口、和存储接口的公知组件。RAM用作处理单元的工作存储器、在非易失性存储器件1100和主机接口之间的高速缓存、以及在非易失性存储器件1100和主机设备之间的缓冲器的至少一个。处理单元控制控制器1200的整体操作。

[0098] 主机接口包括用于在主机设备和控制器1200之间的数据交换的协议。例如，控制器1200可以被配置为使用诸如USB协议、多媒体卡(MMC)协议、PCI协议、PCI-E协议、ATA协议、串行ATA协议、并行ATA协议、SCSI协议、增强小型磁盘接口(ESDI)协议、和集成驱动电子电路(IDE)协议的各种接口协议的至少一个来与外部设备(例如，主机设备)通信。存储器接口与非易失性存储器件1100接口连接。例如，存储器接口包括NAND(与非)快闪接口或NOR(或非)快闪接口。

[0099] 存储系统1000可以进一步包括纠错块(未示出)。纠错块可以被配置为使用纠错码(ECC)来检测和纠正从非易失性存储器件1100读取的数据中的错误。纠错块可以被作为控制器1200的组件而提供。纠错块还可以替换地被提供作为非易失性存储器件1100的组件。

[0100] 可以将控制器1200和非易失性存储器件1100集成为一个半导体设备中。作为例子，可以将控制器1200和非易失性存储器件1100集成为一个半导体设备以形成存储卡。例如，可以将控制器1200和非易失性存储器件1100集成为一个半导体设备，以形成PC卡(例如，个人计算机存储卡国际协会(PCMCIA))、小型快闪卡(CF)、智能媒体卡(SM/SMC)、记忆棒、多媒体卡(例如，MMC、RS-MMC和MMCmicro)、SD卡(例如，SD、miniSD、microSD和SDHC)、或通用快闪存储器(UFS)。

[0101] 作为另一例子，可以将控制器1200和非易失性存储器件1100集成为一个半导体设备中以形成SSD。SSD包括在半导体存储器中存储数据的存储器元件。当存储系统1000被用作SSD时，与硬盘驱动器(HDD)相比，连接至存储系统1000的主机设备的工作速度可以显著增加。

[0102] 以上参照图1至14描述的每个组件表示软件或硬件组件，例如现场可编程门阵列(FPGA)或专用集成电路(ASIC)，但是其不限于此。组件可以有利地被配置为驻留在可寻址存储介质上，并且被配置为在一个或多个处理器上运行。从而，这些组件中具有的功能可以被合并到更少的组件中或者被进一步分成到额外的组件中。

[0103] 现在将参照图15来描述根据本发明的示范性实施例的安全密钥生成方法。

[0104] 可以将根据当前示范性实施例的安全密钥生成方法概括为主机设备获得存储设备的介质ID并且使用介质ID和用户验证信息两者生成安全密钥的过程。

[0105] 参照图15，存储设备存储原始ID(步骤S100)。原始ID可以存储在存储设备的存储器元件中。

[0106] 主机设备接收原始ID(步骤S102)，并且从原始ID计算作为存储设备的唯一标识符的介质ID(步骤S104)。原始ID包括第一原始ID和第二原始ID。可以将第二原始ID被转换为的第二标识符与第一原始ID合并来产生介质ID。可替换地，原始ID自身可以是介质ID。稍后将参照图19至22更加详细地描述计算介质ID的方法。

[0107] 主机设备接收用户验证信息。用户验证信息可以通过用户输入到包括在主机设备中的输入单元(未示出)中，或者可以通过用户输入到除主机设备之外的终端(未示出)，然后提供给主机设备。

[0108] 图16是示出根据本发明的示范性实施例来生成安全密钥并使用安全密钥来加密内容的方法的流程图。在图16中，用于生成安全密钥的步骤S100、S102、S104和S106与图15中所示的那些相同。

[0109] 根据当前示范性实施例的主机设备通过使用安全密钥来加密内容而生成加密的内容，或者将内容转换为加密的内容(步骤S108)。用在内容的加密上的加密算法和加密密钥不限于特定的加密算法和特定的加密密钥。但是，使用相同的密钥来进行加密和解密的对称密钥加密算法，例如，高级加密标准(AES)加密算法可以被使用。

[0110] 向存储设备提供加密的内容(步骤S110)，并且存储设备存储加密的内容(步骤S112)。如图16中所示，主机设备可以在提供原始ID的存储设备中存储加密的内容。从而，存储加密的内容的存储设备不需要不同于提供原始ID的存储设备。

[0111] 参照图16，主机设备不向存储设备提供安全密钥，也不在加密的内容中包括安全密钥。因此，为了获得加密内容的解密密钥，应该获得存储加密内容的存储设备的介质ID，并且应该从介质ID中生成解密密钥。不能直接从存储设备获得加密内容的解密密钥。因此，根据图16的内容加密方法，即使将加密的内容非法复制到另一存储设备，其也不能被解密。

[0112] 现在将参照图19至20更详细地描述主机设备通过其来计算介质ID的方法。

[0113] 图17示出了在其中，存储设备包括第一部分和第二部分，并且存储用于标识第一部分的第一原始ID和用于标识第二部分的第二原始ID的情况中计算介质ID的方法。第一部分和第二部分的每个表示包括在存储设备中的元件或模块，并且也可以是执行特定功能的元件组或模块组。例如，第二部分可以是执行数据存储功能的元件、模块、元件组或模块组，并且第一部分可以是执行控制功能的元件、模块、元件组或模块组。

[0114] 参照图17，主机设备接收第一原始ID和第二原始ID(步骤S114)。

[0115] 主机设备使用第一原始ID和第二原始ID的至少一个来计算介质ID(步骤S116)。当仅使用第一原始ID来计算介质ID时，它可以特定于第一部分。此外，当仅使用第二原始ID来计算介质ID时，它可以特定于第二部分。然而，当使用第一原始ID和第二原始ID两者来计算介质ID时，它可以特定于第一部分和第二部分两者。

[0116] 参照图18，可以将第二原始ID转换为第二标识符(步骤S118)，并且可以使用第一原始ID和第二标识符的至少一个来计算介质ID(步骤S120)。例如，可以使用第一原始ID和第二标识符二者来计算介质ID。

[0117] 当第二部分的唯一标识符不应该被泄漏时，可以向主机设备提供通过加密第二部分的唯一标识符而获得的数据，以作为代替第二部分的唯一标识符的第二原始ID。然后，主

机设备可以使用第二原始ID来生成第二标识符，第二标识符可以用作第二部分的另一标识符。

[0118] 现在将参照科19和20来描述计算介质ID的方法。

[0119] 参照图19，第二部分可以是存储器元件，并且第一部分可以是存储器元件控制器。存储器元件存储其唯一标识符。也可以在存储器元件中存储存储器元件控制器的唯一标识符。

[0120] 首先，将描述生成可以用作存储器元件的另一标识符的存储器导出ID的方法(步骤S10)。存储器导出ID可以被理解为与以上参照图18描述的第二标识符相同。

[0121] 主机设备从存储设备接收通过加密所存储的存储器元件的唯一标识符而获得的加密的存储器ID。加密的存储器ID也可以存储在存储器元件中。加密的存储器ID可以被理解为与以上参照图18描述的第二原始ID相同。

[0122] 主机设备通过解密经加密的存储器ID而生成作为存储器元件的唯一标识符的存储器ID(步骤S124)。

[0123] 主机设备使用存储器ID生成第二验证信息(步骤S126)。具体地，主机设备可以生成随机数，通过加密随机数来生成会话密钥，并且通过将存储器元件的唯一标识符(即，存储器ID)和会话密钥输入到预定的单向函数中而生成第二验证信息。使用单向函数的每个输出值找到单向函数的对应输入值在计算上是不可能的。例如，单向函数可以是使用两个操作数作为输入的逐位运算(bitwise operation)当中的XOR(异或)。

[0124] 存储设备使用存储器ID生成第一验证信息(步骤S128)。除了存储器ID之外，在存储器元件中还可以存储包括多个备用密钥的备用密钥集合。存储设备通过加密备用密钥集合中的一个备用密钥，并且使用由主机设备生成的随机数作为加密密钥来加密备用密钥，从而生成会话密钥。然后，存储设备通过将会话密钥和存储器ID输入到预定的单向函数中可以生成第一验证信息。

[0125] 主机设备从存储设备接收第一验证信息(步骤S130)，并且检验第一验证信息是否匹配于第二验证信息(判决步骤S132)。如果在判决步骤S132中判决第一验证信息不匹配于第二验证信息(判决步骤S132的否分支)，则可以提供验证失败的通知(步骤S134)。

[0126] 如果在步骤S132中检验到第一验证信息匹配于第二验证信息(判决步骤S132的是分支)，则使用存储器元件的唯一标识符(即，存储器ID)来生成存储器导出ID(步骤S136)。可以通过将存储器元件的唯一标识符(即，存储器ID)和专用秘密值(ASSV)输入到预定的单向函数中来生成存储器导出ID。

[0127] 可以将ASSV赋予在主机设备上运行的每个应用。例如，可以向音乐记录应用、视频记录应用、和软件记录应用赋予不同的ASSV。对于加密的内容的每种类型，或者对于加密的内容的每个提供商ID，ASSV可以具有唯一值。优选地，对于加密的内容的每种类型，ASSV可以具有唯一值。例如，内容的类型可以是内容是视频、音乐、文档、或者是软件。

[0128] 接下来，将描述一种接收存储器元件控制器的唯一标识符(即，控制器ID)的方法(步骤S20)。

[0129] 具体地，现在将参照图20来描述主机设备通过其从存储设备接收存储器元件控制器的唯一标识符(即，控制器ID)的方法(步骤S20)。

[0130] 参照图20，主机设备从存储设备接收第三验证信息(步骤S140)。如上所述，第三验

证信息可以包括存储设备的验证证书和包括在存储设备中的控制器的控制器ID。

[0131] 主机设备和存储设备可以彼此相互验证(步骤S141)。此相互验证可以是基于公钥的验证。当相互验证失败时(判决步骤S142的否分支),主机设备提供验证失败的通知(步骤S144)。当相互验证成功时(判决的是分支),主机设备可以从第三验证信息获得控制器ID(步骤S148)。

[0132] 主机设备使用存储器导出ID和控制器ID的至少一个来计算介质ID。优选地,主机设备使用存储器导出ID和控制器ID两者来计算介质ID。

[0133] 可以作为在存储器导出ID和控制器ID上执行二元运算的结果来获得介质ID。例如,可以作为在存储器导出ID和控制器ID上执行需要两个操作数的二元运算(诸如AND(与)、OR(或)、XOR(异或)等)的结果来获得介质ID。

[0134] 可以作为按如下次序执行STRCAT运算(即,连接存储器导出ID和控制器ID)的结果来获得介质ID。或者,可以作为按如下次序执行STRCAT运算(即,连接控制器ID和存储器导出ID)的结果来获得介质ID。

[0135] 现在将参照图21来描述根据本发明的示范性实施例生成安全密钥并使用安全密钥来解密内容的方法。

[0136] 参照图21,在存储设备中存储原始ID和加密的内容(步骤S200和S201)。假设通过利用如下的加密密钥来加密内容而生成加密的内容,其中使用存储设备的介质ID和用户验证信息A(密码A)而生成所述加密密钥。

[0137] 主机设备从存储设备接收原始ID(步骤S202)。虽然图21中未示出,但是主机设备可以请求存储设备提供原始ID,并且接收响应于请求的原始ID。主机设备当从用户接收播放加密的内容的命令时,可以作出对原始ID的请求。

[0138] 主机设备使用原始ID计算介质ID(步骤S203)。主机设备的介质ID计算操作可以与以上参照图17至20描述的主机设备的介质ID计算操作相同,从而将省略其重复描述。

[0139] 主机设备从用户接收验证信息(密码A)(步骤S204)。所接收的验证信息可以相同或不同于用来生成用于加密的内容的加密密钥的验证信息。为便于描述,假设所接收的验证信息与用来生成用于加密的内容的加密密钥的验证信息相同。

[0140] 主机设备使用介质ID和验证信息生成解密密钥(步骤S205)。

[0141] 可以仅使用介质ID和验证信息来执行解密密钥的生成,或者除了介质ID和验证信息之外还使用一个或多个变量或常量数据来执行解密密钥的生成(步骤S205)。

[0142] 例如,解密密钥可以是作为在介质ID和验证信息上执行二元运算的结果而产生的数据。特别地,解密密钥可以是作为执行XOR(异或)运算的结果产生的数据。从而,解密密钥可以是作为在介质ID和验证信息上执行XOR(异或)运算的结果而获得的数据。

[0143] 解密密钥还可以是作为在介质ID和验证信息上执行STRCAT运算的结果而产生的数据。在STRCAT运算中,可以按任何次序连接串。因此,可以按此次序或相反次序来连接介质ID和验证信息。

[0144] 主机设备读取存储在存储设备中的加密内容(步骤S206),使用解密密钥解密经加密的内容(步骤S207),并且播放解密的内容(步骤S208)。

[0145] 现在将参照图22来描述主机设备不能解密从内容存储设备X(200)非法复制到内容存储设备Y(201)的经加密的内容的过程。

[0146] 参照图22，在内容存储设备Y(201)中存储不同于存储在内容存储设备X(200)中的原始ID的原始ID Y(步骤S210)。

[0147] 此外，在内容存储设备X(200)中存储在复制之前获得的、通过使用图16的加密方法来加密内容而创建的加密的内容(步骤S209)。假设用于生成加密密钥XA的验证信息是A(密码A)。此外，假设用户从内容存储设备X(200)向内容存储设备Y(201)非法复制加密的内容(步骤S211)。

[0148] 当用户将内容存储设备Y(201)连接至主机设备，并且向主机设备输入用于播放加密的内容的命令时，内容存储设备存储加密的内容(步骤S212)，主机设备接收存储在内容存储设备Y(201)中的原始ID Y(步骤S213)。

[0149] 主机设备使用原始ID Y生成内容存储设备Y(201)的介质ID(步骤S214)。

[0150] 主机设备接收用户验证信息(步骤S215)。假设用户验证信息是与用来生成用于加密的内容的加密密钥XA的验证信息A一样的A(密码A)。

[0151] 主机设备使用介质ID和用户验证信息A生成解密密钥YA(步骤S216)。

[0152] 主机设备试图使用所生成的解密密钥YA来解密从内容存储设备Y(201)接收(步骤S217)的加密内容(步骤S218)。然而，因为在步骤S216中生成的解密密钥YA不同于加密内容的解密密钥XA，所以主机设备不能解密经加密的内容。

[0153] 因此，主机设备不能够播放非法复制到并存储在内容存储设备Y(201)中的经加密的内容(步骤S219)。

[0154] 在图22中，假设用户输入正确的验证信息(例如，与用来生成加密密钥XA的用户验证信息A一样的验证信息)。然而，即使用户输入不正确的验证信息，即，不同于用来生成加密密钥XA的用户验证信息A的验证信息，主机设备也不能播放非法复制到并存储在内容存储设备Y(201)中的经加密的内容(步骤S219)。

[0155] 从而，不管是否输入正确的用户验证信息，都不能够播放非法复制到并存储在内容存储设备Y(201)中的加密内容。

[0156] 图23示出其中当用来生成用于加密的内容的加密密钥的用户验证信息不正确时，主机设备不能播放经加密的内容的示范性实施例。

[0157] 参照图23，内容存储设备X(200)存储通过利用加密密钥XA加密内容而获得的加密的内容(步骤S209)，其中，使用内容存储设备X(200)的介质ID和第一用户验证信息A(密码A)来生成加密密钥XA。第一验证信息用于生成用于加密的内容的加密密钥XA。加密密钥XA还可以用作用于解密经加密的内容的解密密钥。

[0158] 当第二用户将内容存储设备X(200)连接至主机设备，并且向主机设备输入用于播放加密的内容的命令时，主机设备接收存储在内容存储设备X(200)中的原始ID X。

[0159] 主机设备使用原始ID X来生成内容存储设备X(200)的介质ID(步骤S221)。

[0160] 主机设备从第二用户接收第二用户验证信息B(密码B)(步骤S222)。假设第二用户验证信息是不同于第一验证信息A的B，其中，所述第一验证信息A用来生成用于加密的内容的加密密钥XA。

[0161] 主机设备使用介质ID和第二用户验证信息B生成解密密钥XB(步骤S223)。

[0162] 主机设备试图使用所生成的解密密钥XB来解密从内容存储设备X(200)接收(操作S224)的加密的内容(步骤S225)。然而，因为所生成的解密密钥XB不同于经加密的内容的解

密密钥XA，所以主机设备不能解密经加密的内容。

[0163] 因此，主机设备不能够播放存储在内容存储设备X(200)中的经加密的内容(步骤S219)。

[0164] 在图23中，假设主机设备的用户是不同于第一用户的第二用户，或者是输入不正确的验证信息(例如，不同于用来生成加密密钥XA的用户验证信息A的验证信息)的相同的第一用户。然而，如果第二用户输入正确的验证信息，即，与用来生成加密密钥XA的第一用户验证信息A相同的验证信息，则主机设备可以播放加密的内容。

[0165] 本发明可以生成属于特定设备和特定用户两者的安全密钥。例如，使用通过根据本发明的安全密钥生成装置生成的安全密钥来加密的内容仅当与安全密钥的生成有关的特定用户使用特定设备时才能被解密。

[0166] 此外，当安全密钥生成装置支持信赖的计算时，它在支持信赖的计算环境的安全模式下生成安全密钥。因此，可以防止诸如用户验证信息、设备ID、和所生成的安全密钥的信息的泄漏(例如，被盗)。

[0167] 本领域技术人员将理解，可以在不实质脱离本发明的原则的情况下对示范性实施例进行很多变化和修改。因此，所公开的本发明的示范性实施例仅用在普通的和描述的意义，而不用于限制的目的。

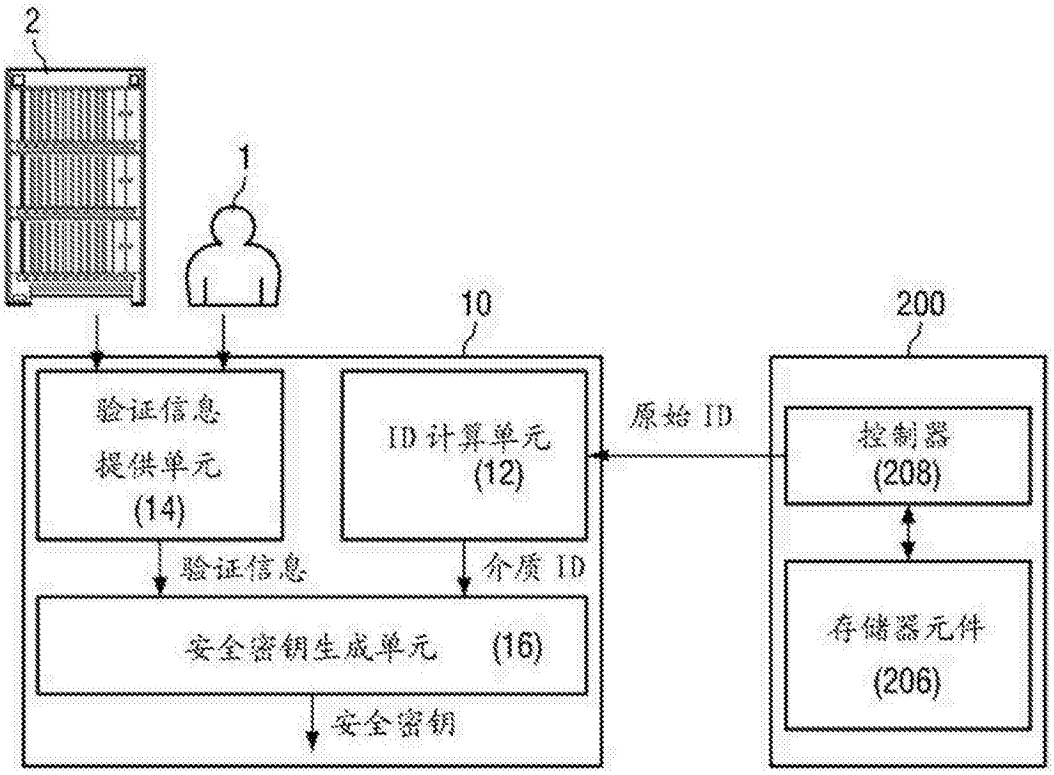

2
1
10
200
验证信息
提供单元
(14)
ID 计算单元
(12)
原始 ID
控制器
(208)
验证信息
介质 ID
安全密钥生成单元 (16)
存储器元件
(206)
安全密钥

图1

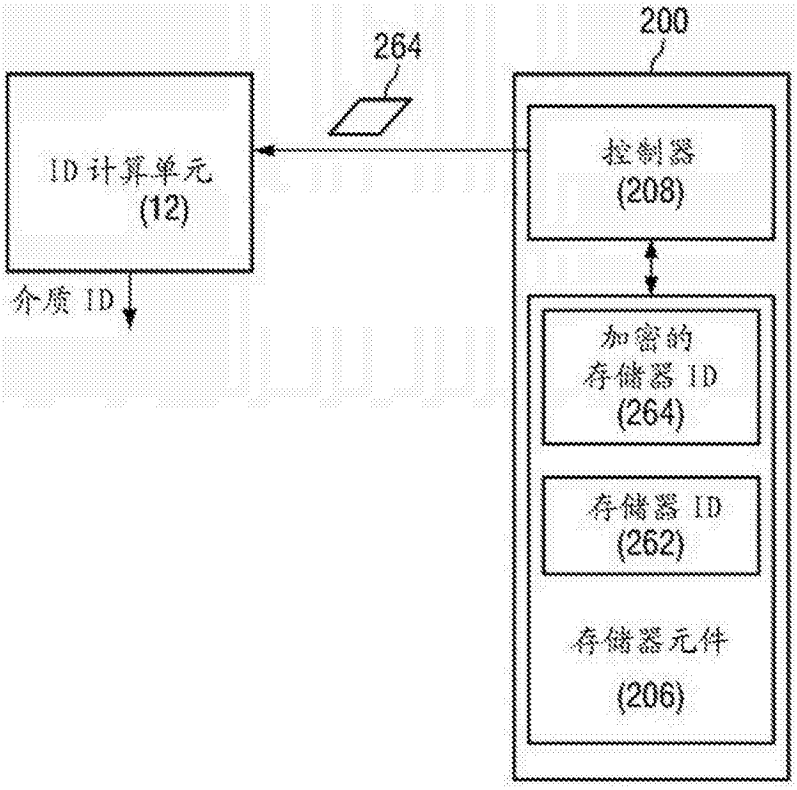

200
264
ID 计算单元
(12)
控制器
(208)
介质 ID
加密的
存储器 ID
(264)
存储器 ID
(262)
存储器元件
(206)

图2

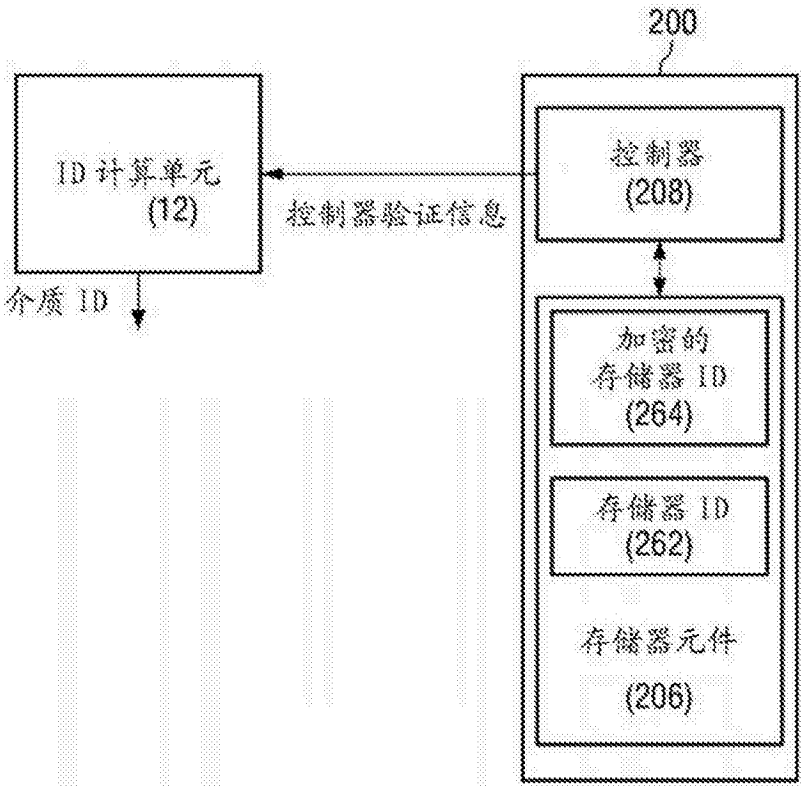

200
ID 计算单元
(12)
控制器验证信息
控制器
(208)
介质 ID
加密的
存储器 ID
(264)
存储器 ID
(262)
存储器元件
(206)

图3

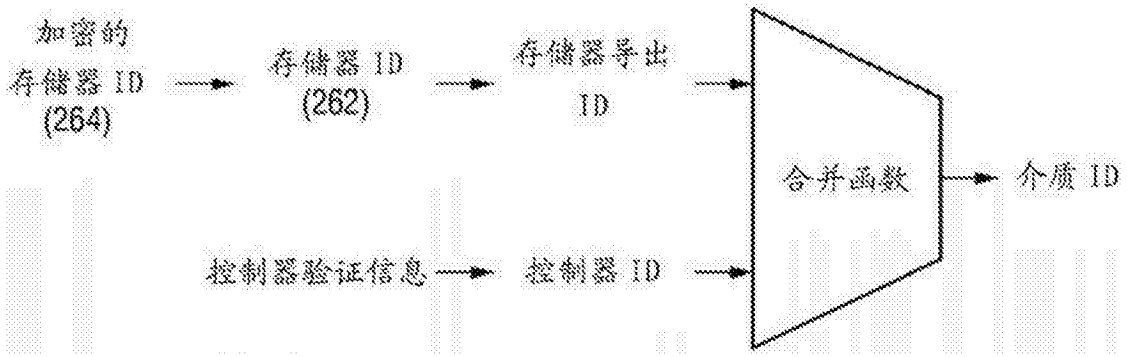

加密的
存储器 ID
(264)
存储器 ID
(262)
存储器导出
ID
控制器验证信息
控制器 ID
合并函数
介质 ID

图4

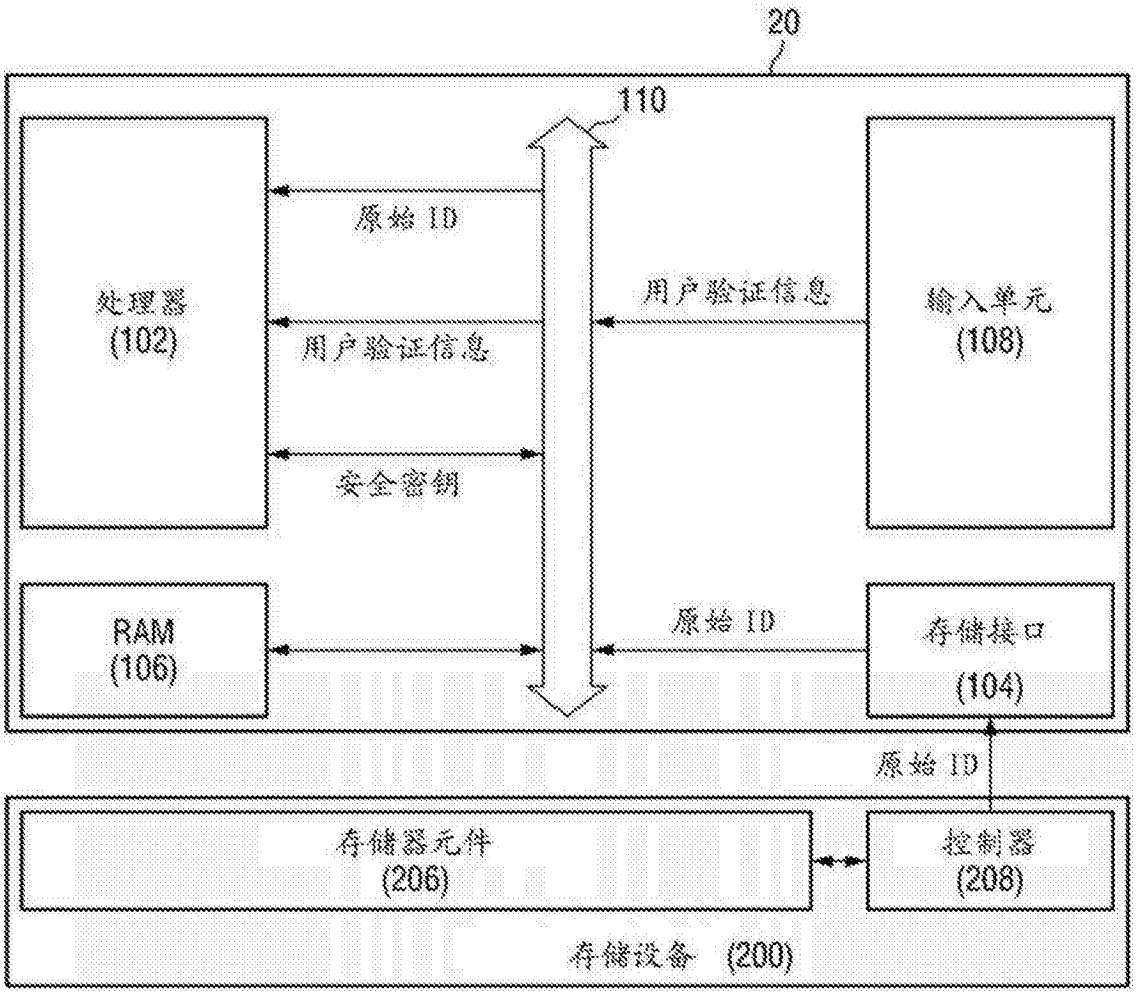

20
110
处理器
(102)
原始 ID
用户验证信息
安全密钥
用户验证信息
输入单元
(108)
RAM
(106)
原始 ID
存储接口
(104)
原始 ID
存储器元件
(206)
控制器
(208)
存储设备 (200)

图5

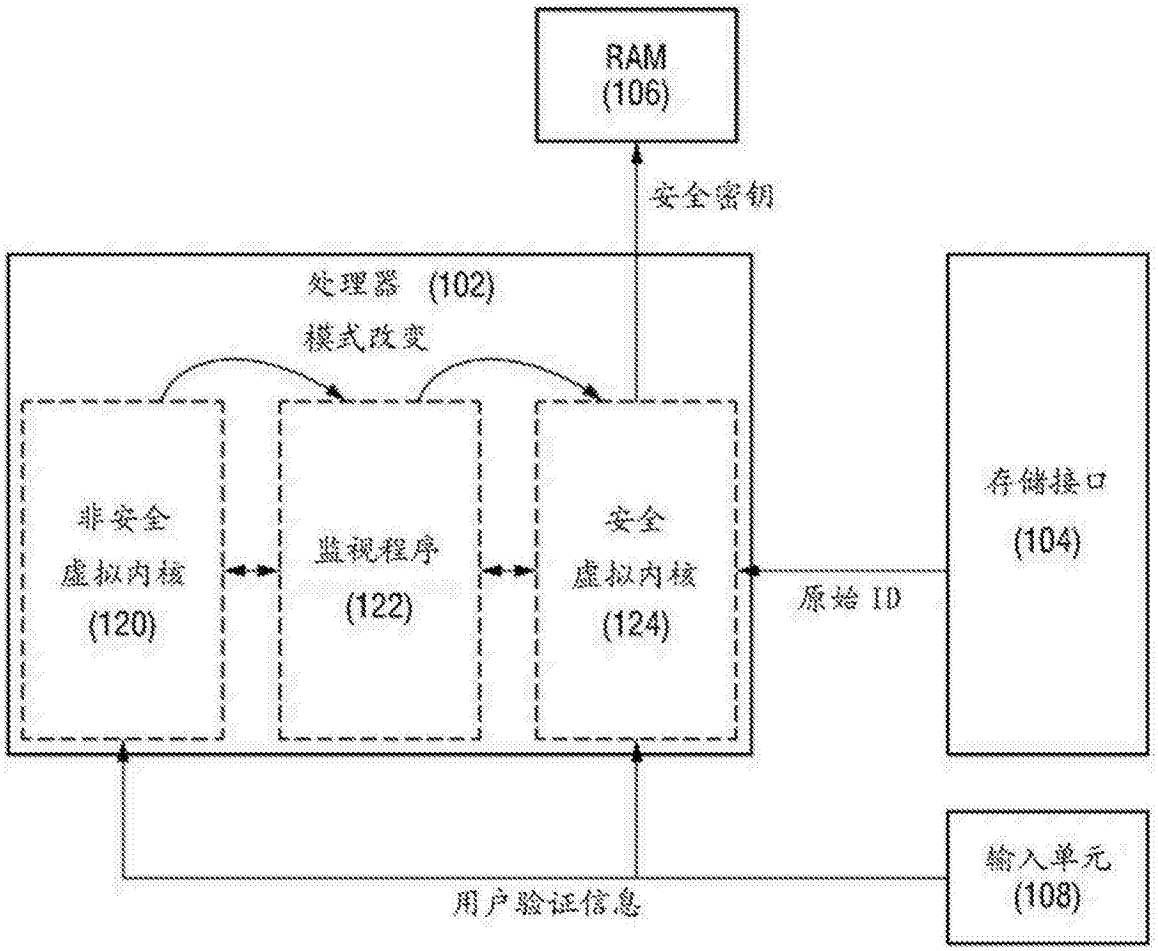

RAM
(106)
安全密钥
处理器 (102)
模式改变
非安全
虚拟内核
(120)
监视程序
(122)
安全
虚拟内核
(124)
原始 ID
存储接口
(104)
输入单元
(108)
用户验证信息

图6

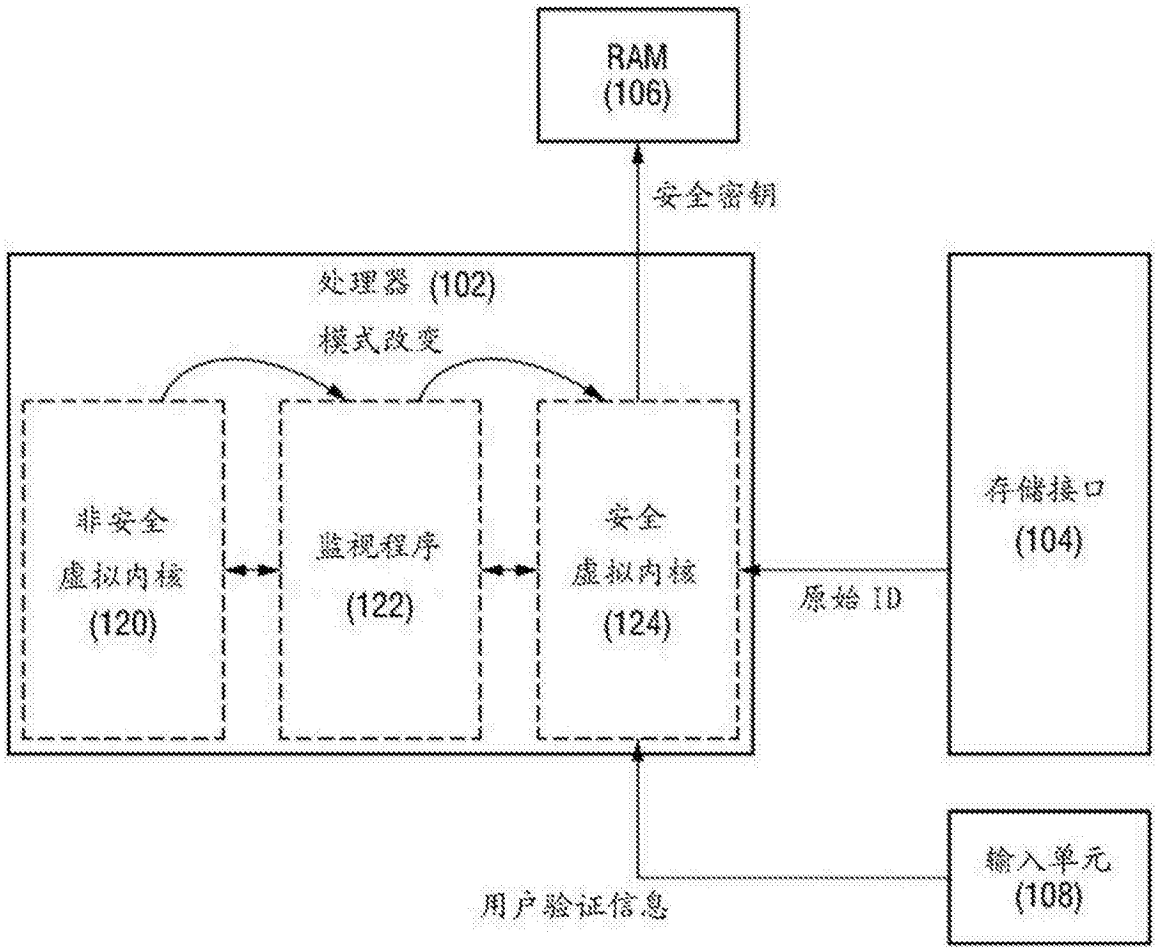

RAM
(106)
安全密钥
处理器 (102)
模式改变
非安全
虚拟内核
(120)
监视程序
(122)
安全
虚拟内核
(124)
原始 ID
存储接口
(104)
输入单元
(108)
用户验证信息

图7

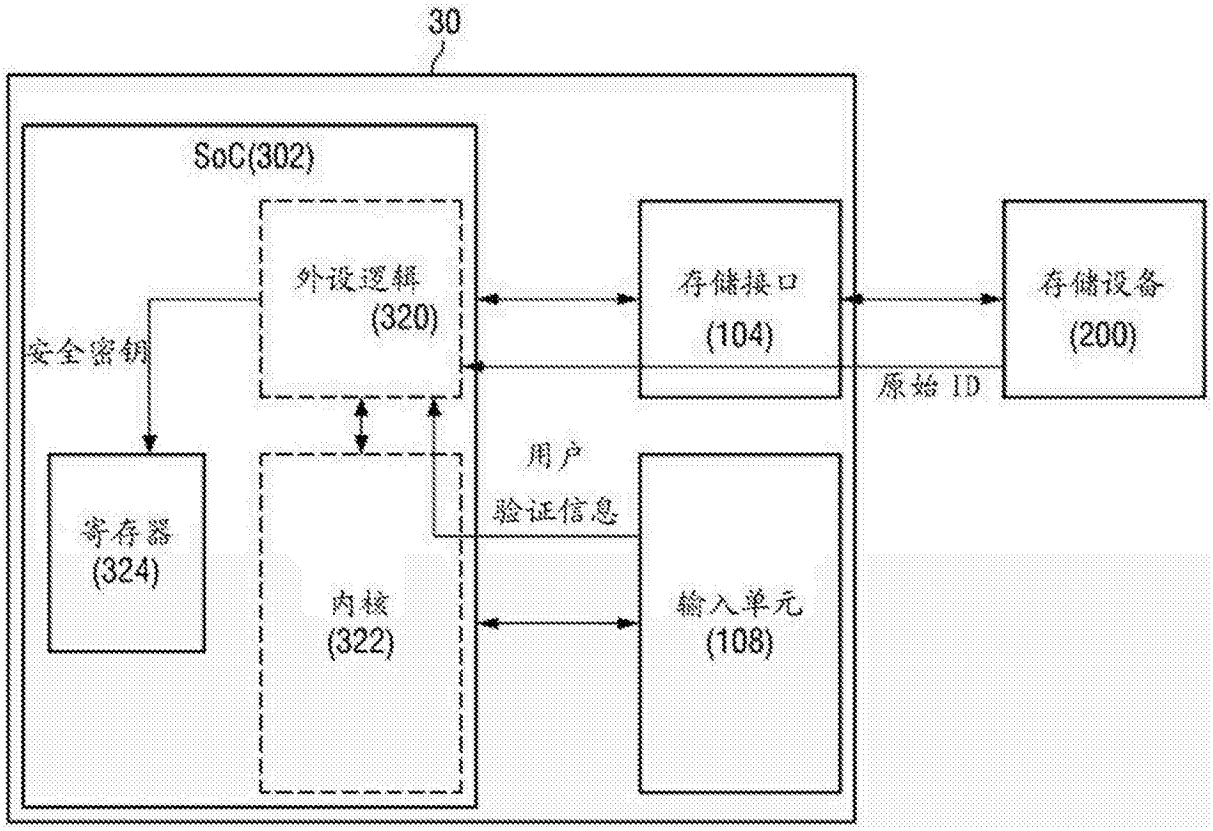

30
SoC(302)
外设逻辑
(320)
存储接口
(104)
存储设备
(200)
安全密钥
原始 ID
用户
验证信息
寄存器
(324)
内核
(322)
输入单元
(108)

图8

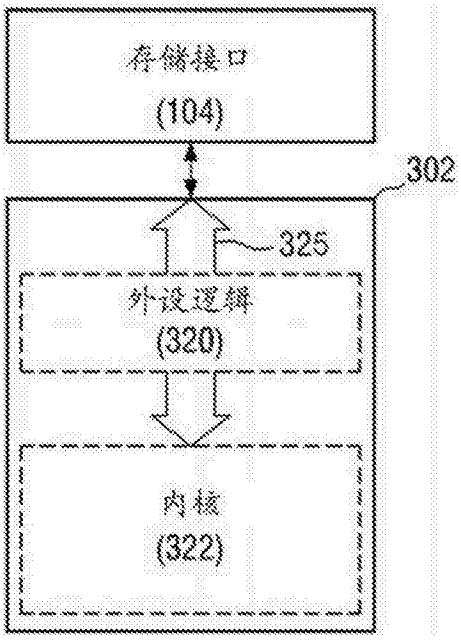

存储接口
(104)
302
325
外设逻辑
(320)
内核
(322)

图9

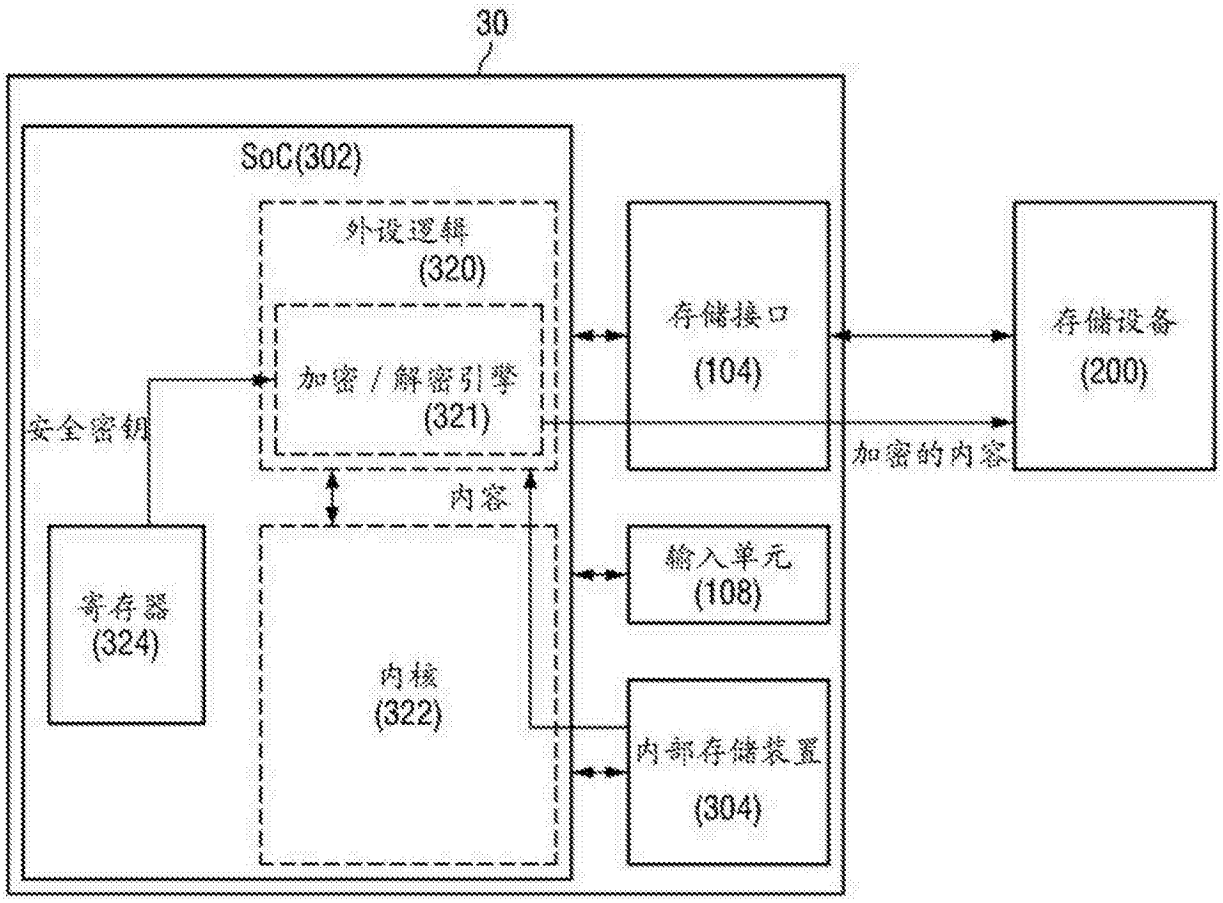

30
SoC(302)
外设逻辑
(320)
加密/解密引擎
(321)
存储接口
(104)
存储设备
(200)
安全密钥
加密的内容
内容
寄存器
(324)
内核
(322)
输入单元
(108)
内部存储装置
(304)

图10

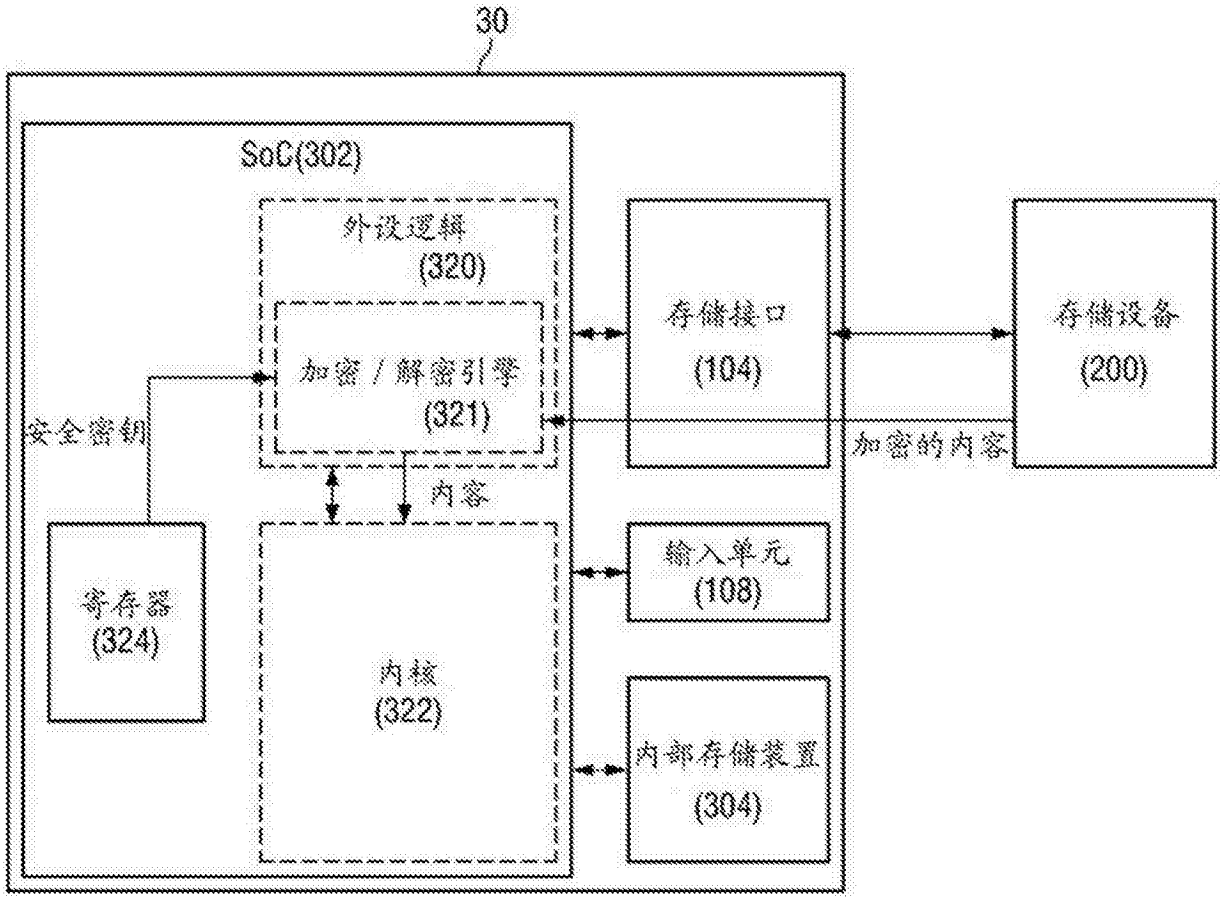

30
SoC(302)
外设逻辑
(320)
加密 / 解密引擎
(321)
安全密钥
内容
寄存器
(324)
内核
(322)
存储接口
(104)
存储设备
(200)
加密的内容
输入单元
(108)
内部存储装置
(304)

图11

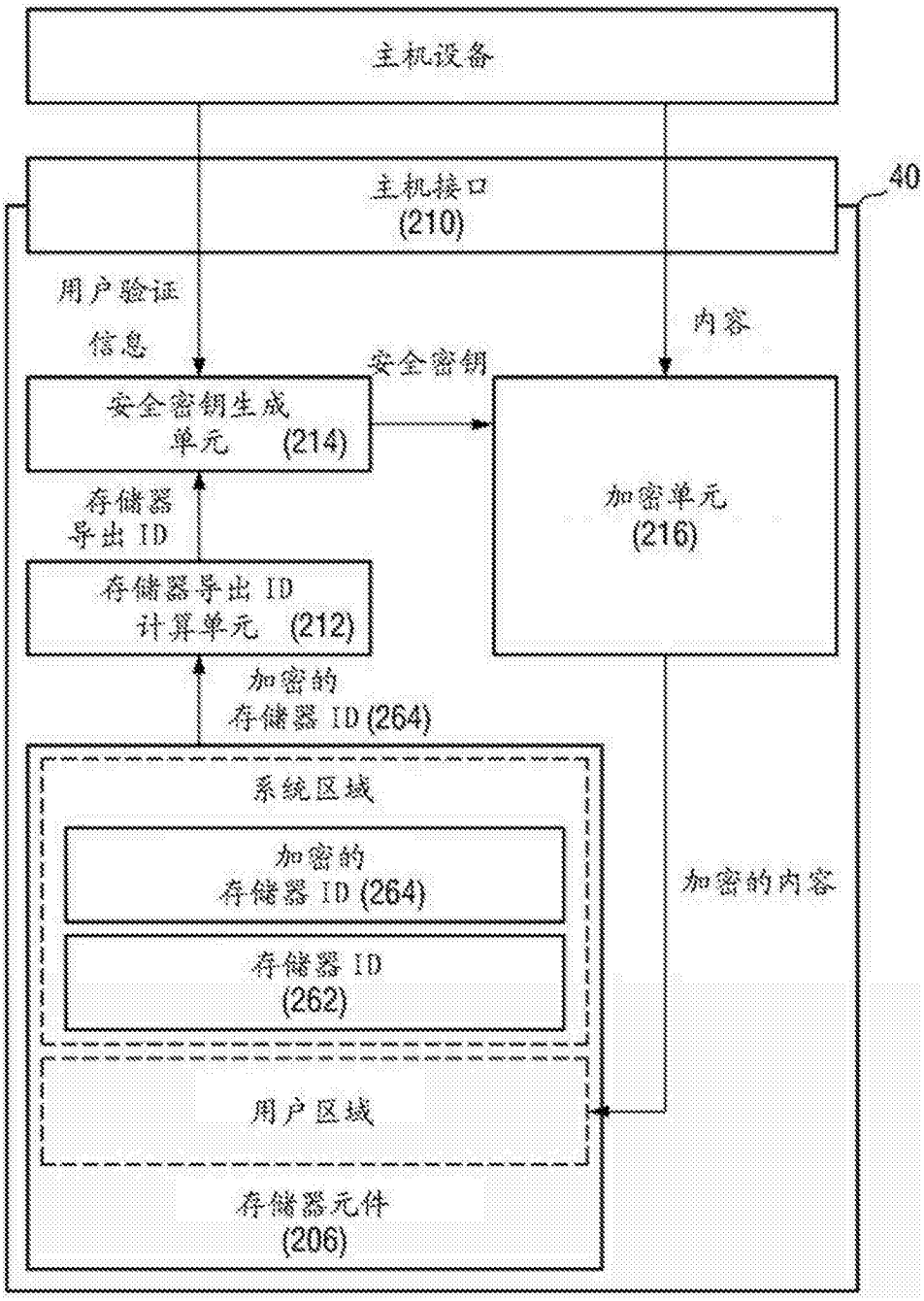

主机设备
主机接口
(210)
40
用户验证
信息
内容
安全密钥
安全密钥生成
单元 (214)
加密单元
(216)
存储器
导出 ID
存储器导出 ID
计算单元 (212)
加密的
存储器 ID (264)
系统区域
加密的
存储器 ID (264)
存储器 ID
(262)
加密的内容
用户区域
存储器元件
(206)

图12

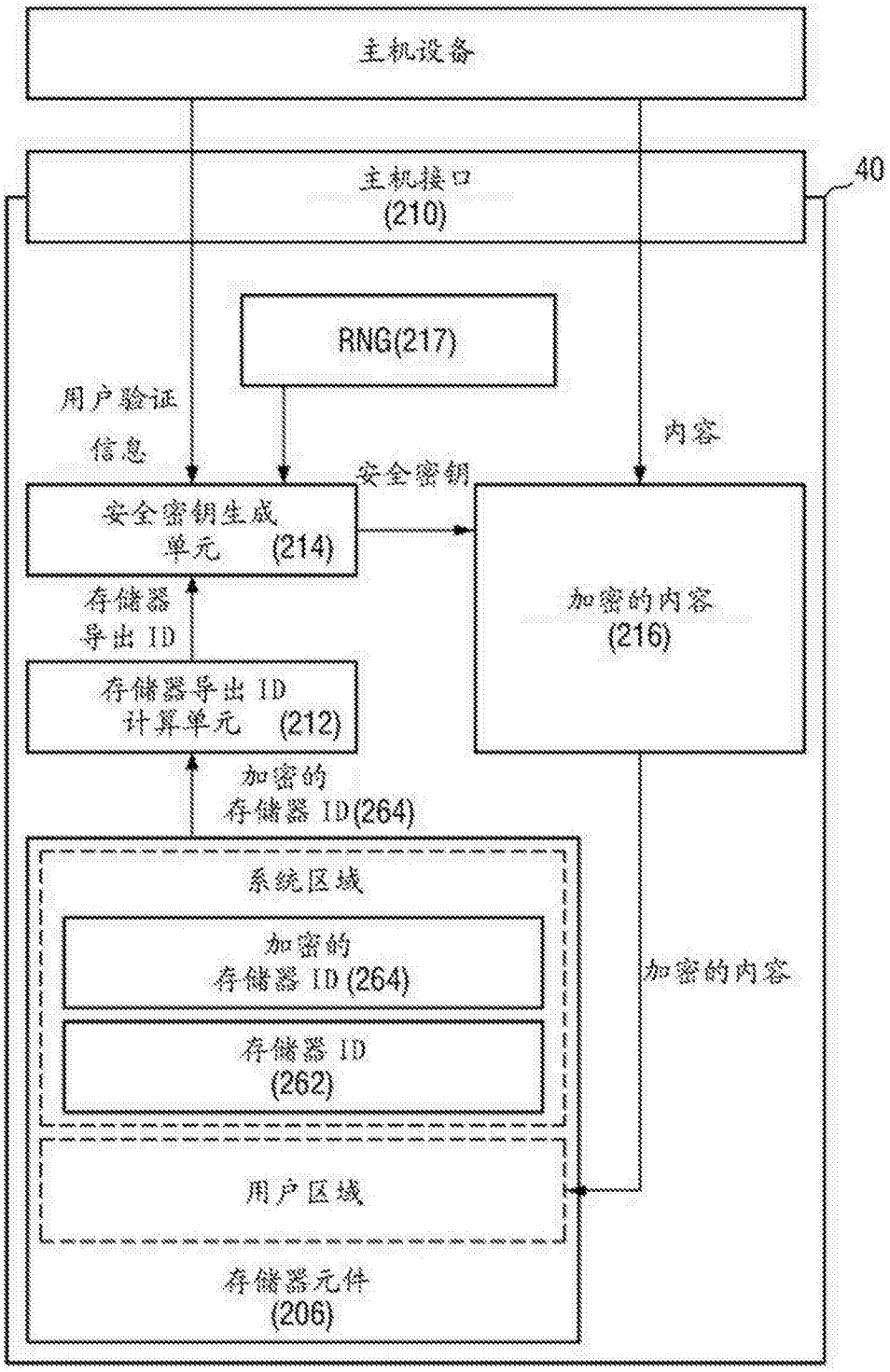

主机设备
主机接口
(210)
40
RNG(217)
用户验证
信息
内容
安全密钥
安全密钥生成
单元 (214)
加密的内容
(216)
存储器
导出 ID
存储器导出 ID
计算单元 (212)
加密的
存储器 ID(264)
系统区域
加密的
存储器 ID (264)
存储器 ID
(262)
加密的内容
用户区域
存储器元件
(206)

图13

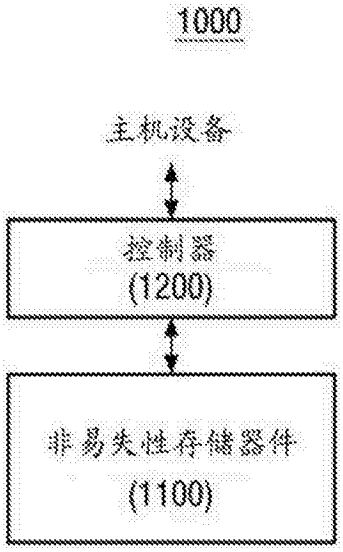

1000
主机设备
控制器
(1200)
非易失性存储器件
(1100)

图14

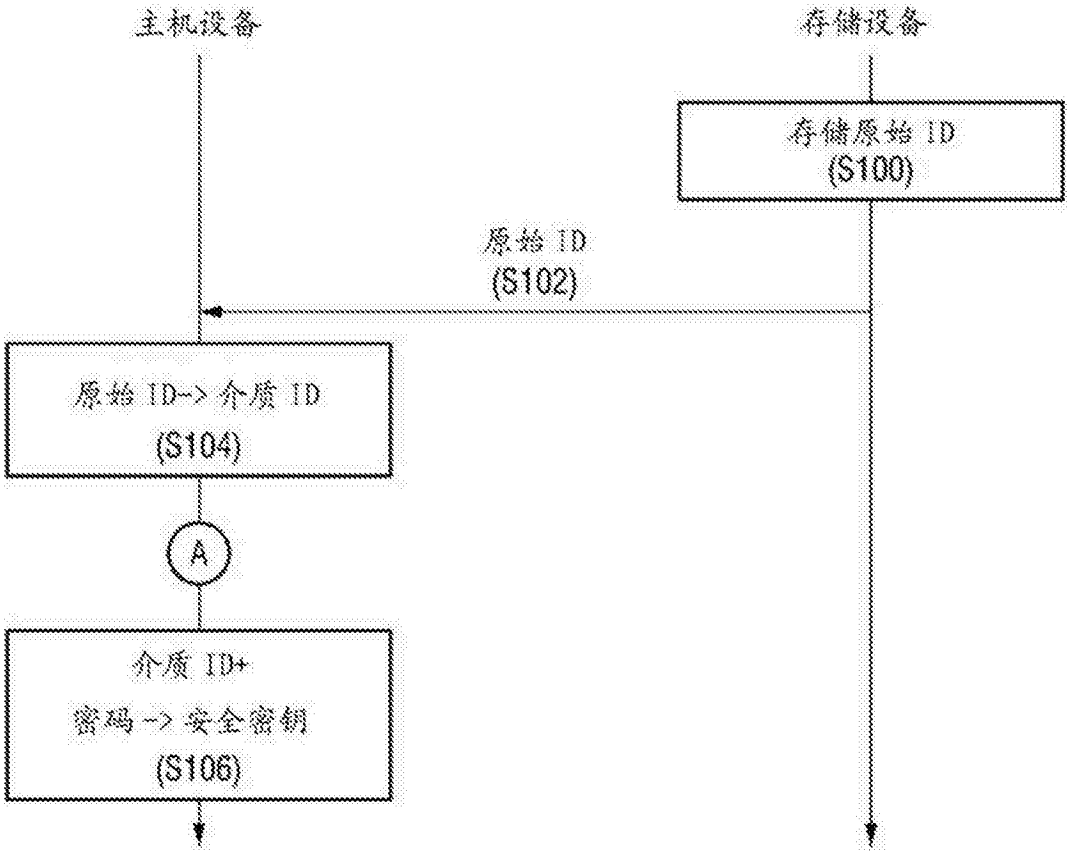

主机设备
存储设备
存储原始 ID
(S100)
原始 ID
(S102)
原始 ID-> 介质 ID
(S104)
A
介质 ID+
密码 -> 安全密钥
(S106)

图15

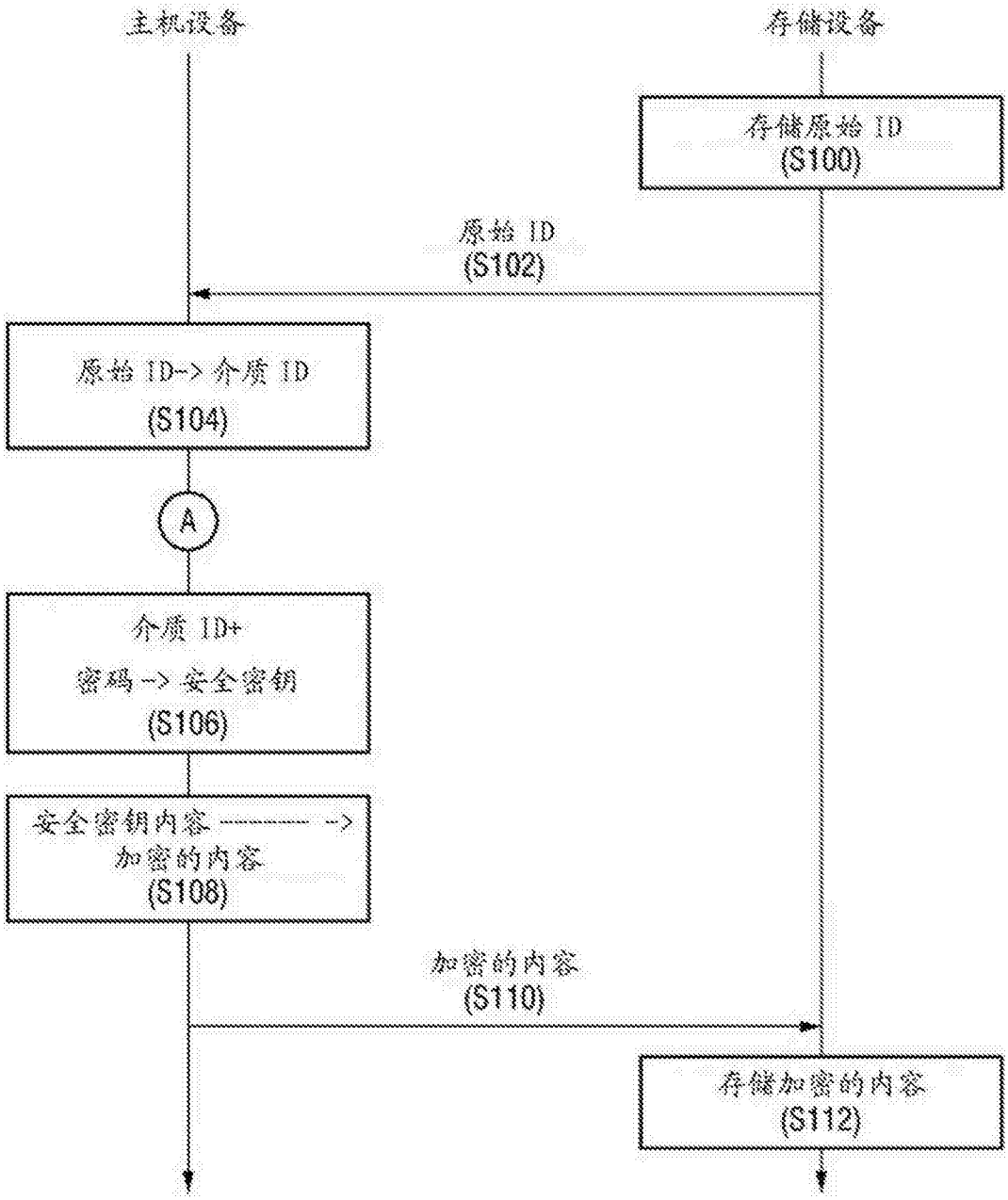

主机设备
存储设备
存储原始 ID
(S100)
原始 ID
(S102)
原始 ID-> 介质 ID
(S104)
A
介质 ID+
密码 -> 安全密钥
(S106)
安全密钥内容 ——— ->
加密的内容
(S108)
加密的内容
(S110)
存储加密的内容
(S112)

图16

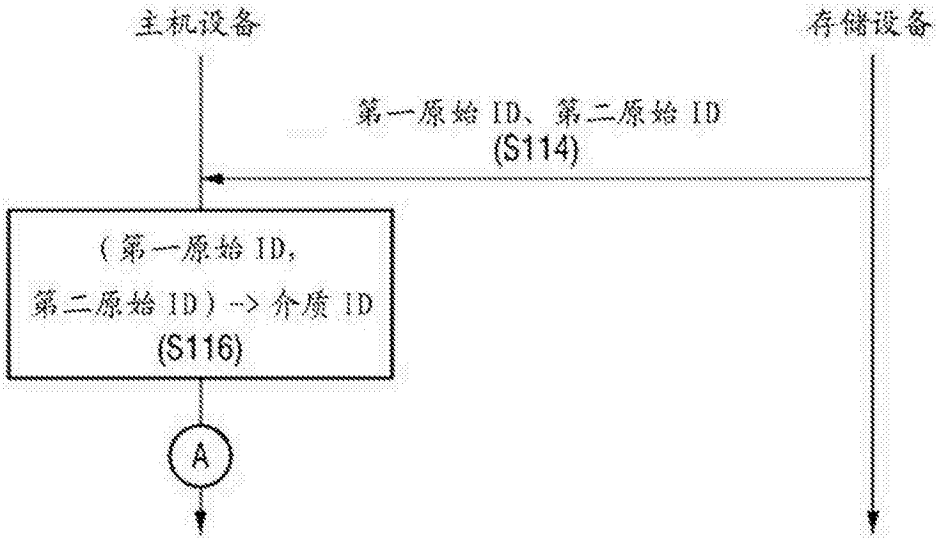

主机设备
存储设备
第一原始 ID、第二原始 ID
(S114)
(第一原始 ID,
第二原始 ID) -> 介质 ID
(S116)
A

图17

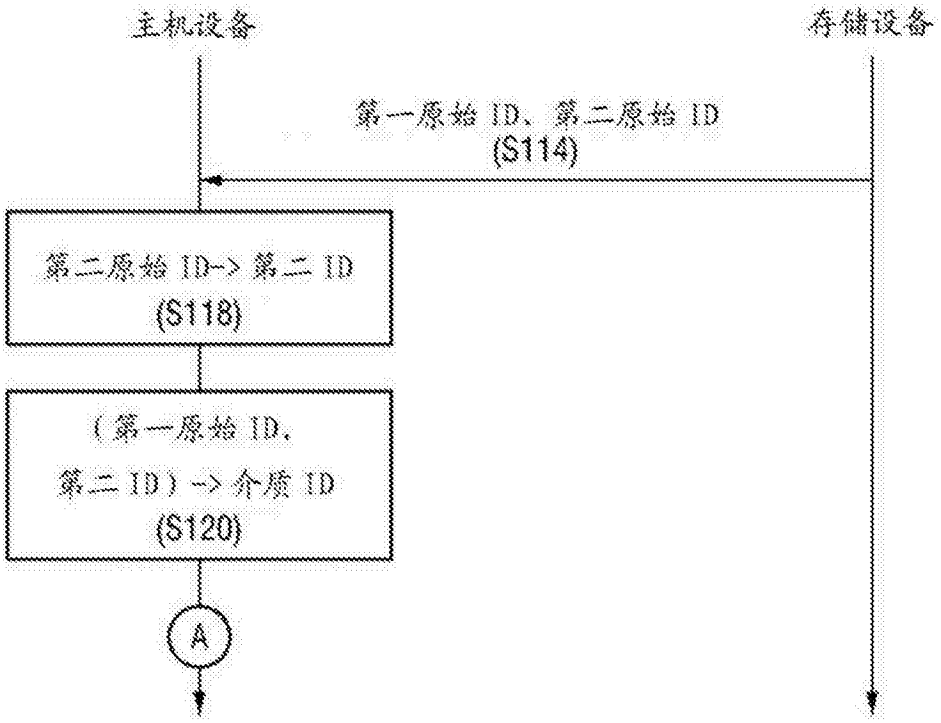

主机设备
存储设备
第一原始 ID、第二原始 ID
(S114)
第二原始 ID-> 第二 ID
(S118)
(第一原始 ID,
第二 ID) -> 介质 ID
(S120)
A

图18

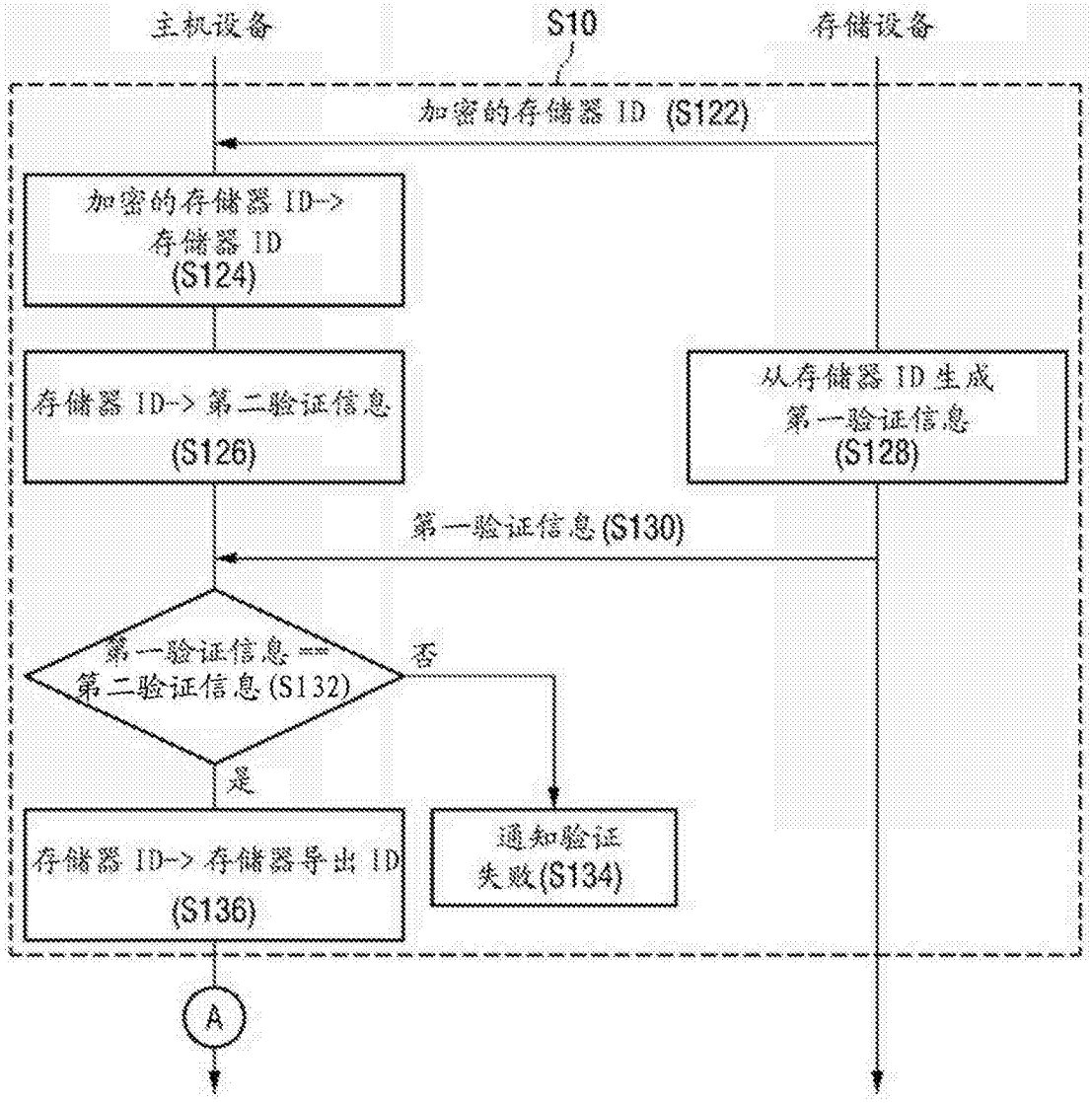

主机设备
S10
存储设备
加密的存储器 ID (S122)
加密的存储器 ID-> 存储器 ID (S124)
存储器 ID-> 第二验证信息 (S126)
从存储器 ID 生成 第一验证信息 (S128)
第一验证信息 (S130)
第一验证信息 == 第二验证信息 (S132)
否
是
通知验证失败 (S134)
存储器 ID-> 存储器导出 ID (S136)
A

图19

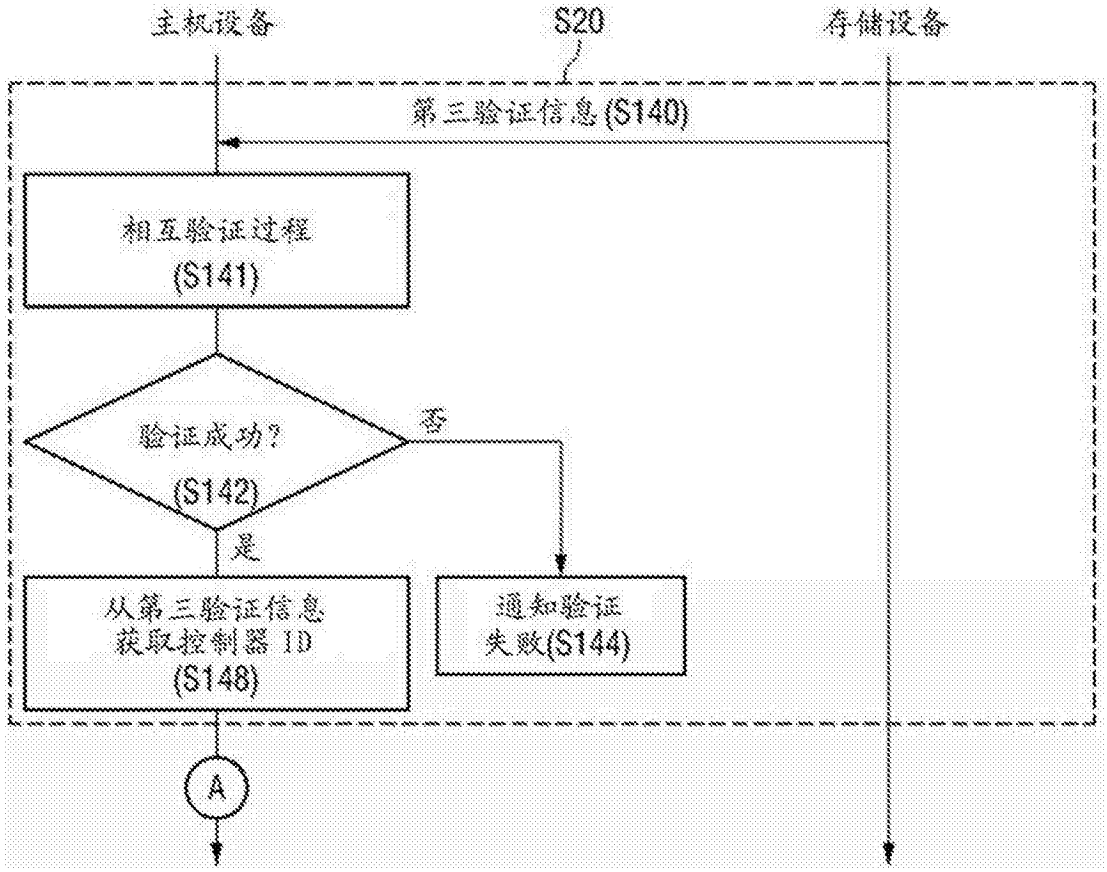

主机设备
S20
存储设备
第三验证信息(S140)
相互验证过程
(S141)
验证成功?
(S142)
否
是
从第三验证信息
获取控制器 ID
(S148)
通知验证
失败(S144)
A

图20

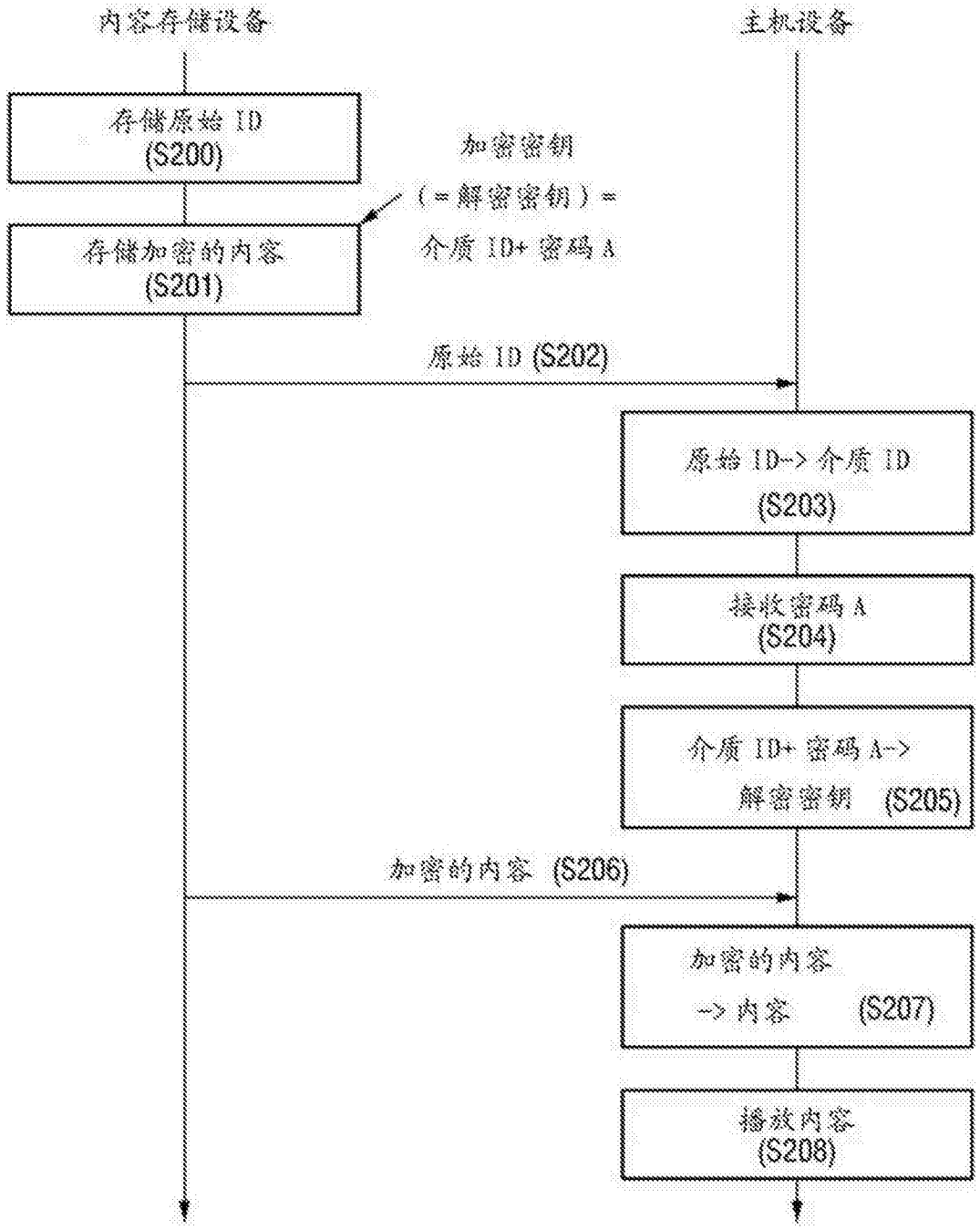

内容存储设备
主机设备
存储原始 ID
(S200)
加密密钥
(=解密密钥)=
介质 ID+ 密码 A
存储加密的内容
(S201)
原始 ID (S202)
原始 ID-> 介质 ID
(S203)
接收密码 A
(S204)
介质 ID+ 密码 A->
解密密钥 (S205)
加密的内容 (S206)
加密的内容
-> 内容 (S207)
播放内容
(S208)

图21

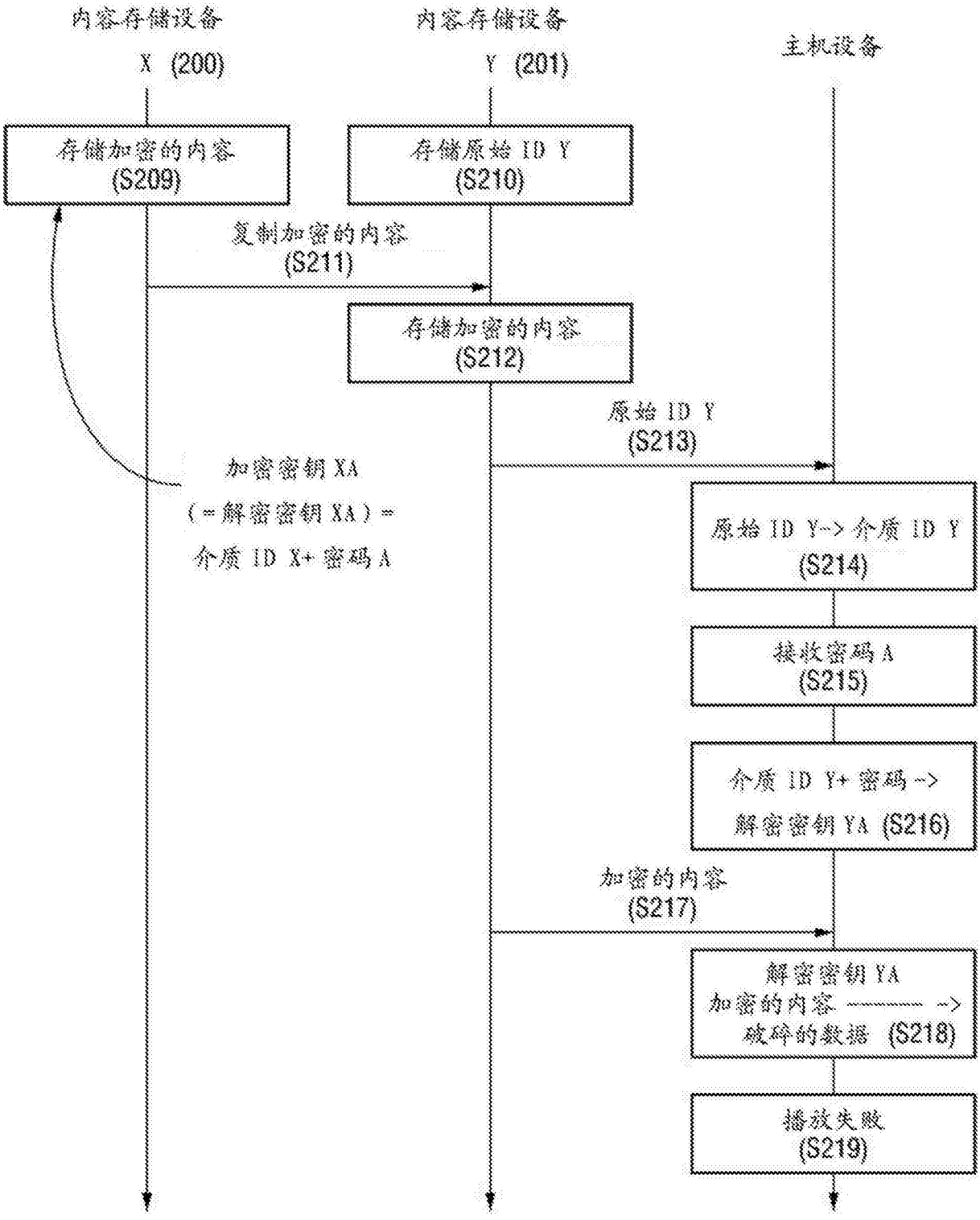

内容存储设备
X (200)
内容存储设备
Y (201)
主机设备
存储加密的内容
(S209)
存储原始 ID Y
(S210)
复制加密的内容
(S211)
存储加密的内容
(S212)
原始 ID Y
(S213)
加密密钥 XA
(=解密密钥 XA)=
介质 ID X+密码 A
原始 ID Y-> 介质 ID Y
(S214)
接收密码 A
(S215)
介质 ID Y+密码 ->
解密密钥 YA (S216)
加密的内容
(S217)
解密密钥 YA
加密的内容 ——— ->
破碎的数据 (S218)
播放失败
(S219)

图22

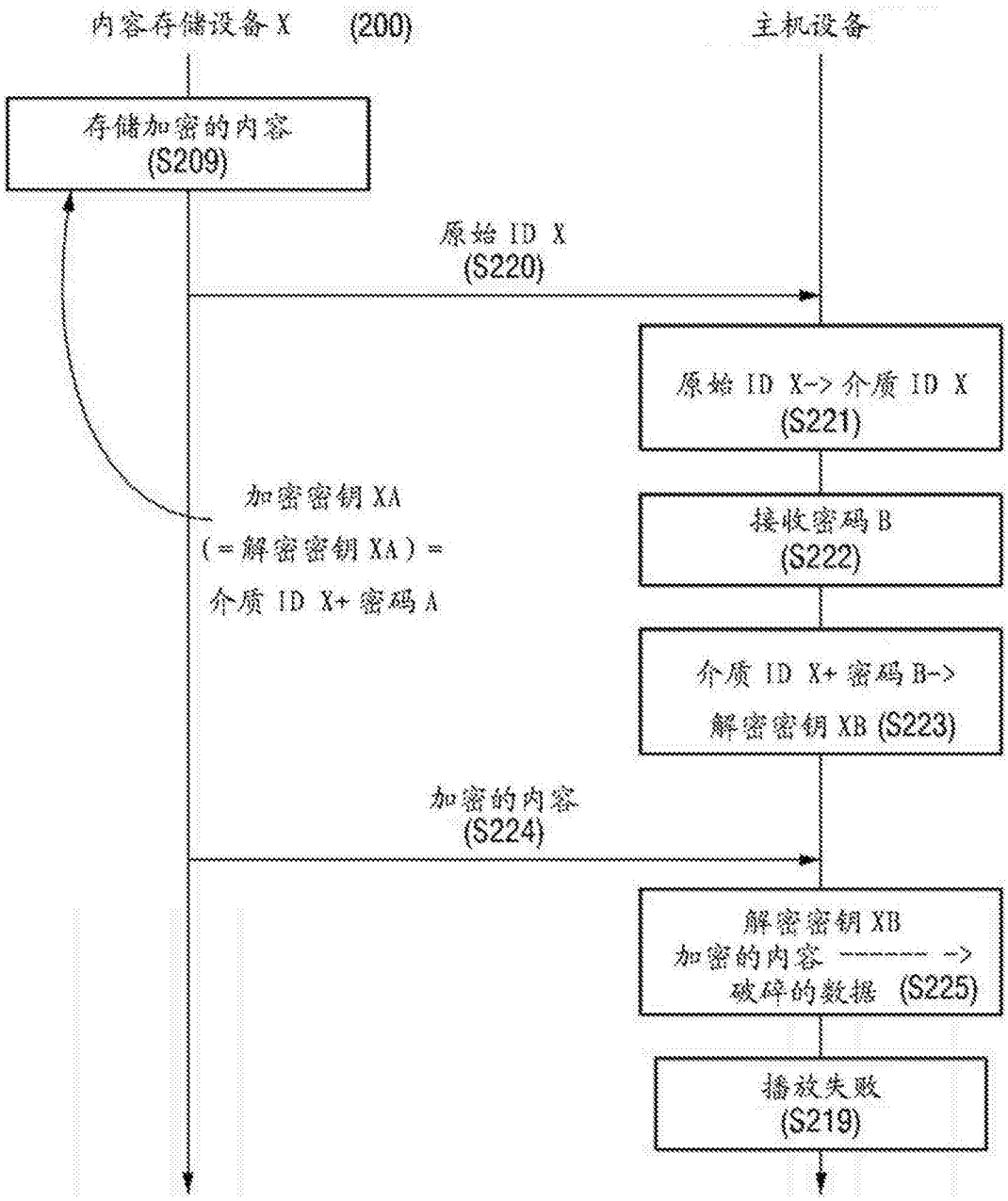

内容存储设备 X (200)
主机设备
存储加密的内容 (S209)
原始 ID X (S220)
原始 ID X-> 介质 ID X (S221)
加密密钥 XA
(=解密密钥 XA) =
介质 ID X+ 密码 A
接收密码 B (S222)
介质 ID X+ 密码 B-> 解密密钥 XB (S223)
加密的内容 (S224)
解密密钥 XB
加密的内容 ——— ->
破碎的数据 (S225)
播放失败 (S219)

图23