[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610159594.6

[43] 公开日 2007 年 10 月 3 日

[11] 公开号 CN 101047495A

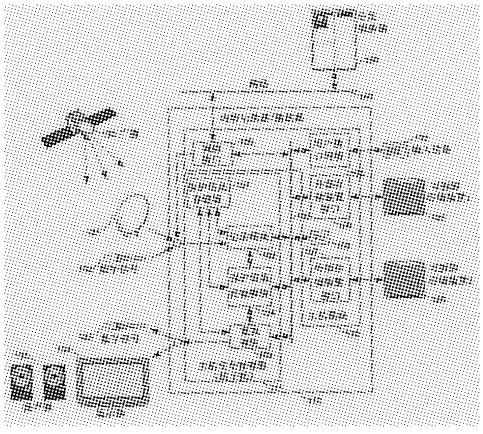
[22] 申请日 2006.9.28
[21] 申请号 200610159594.6
[30] 优先权
[32] 2005. 9.29 [33] JP [31] 2005 - 283878
[71] 申请人 日立环球储存科技荷兰有限公司
地址 荷兰阿姆斯特丹
[72] 发明人 平井达哉 高野晴子
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 李 涛 钟 强
权利要求书 8 页 说明书 90 页 附图 23 页

[54] 发明名称

用于传送数据的方法和系统

[57] 摘要

本发明是用于在设备之间传送密钥数据和相关控制信息并减少加密计算负荷的系统和方法，包括：第一设备，用于记录/再生内容数据；第二设备，用于存储内容数据；主处理器，用于控制该两个设备之间的数据传送。 主处理器用于控制系统以查询两个设备内部数据的传送功能，然后根据查询结果在数据传送之前，设立从第一设备向第二设备单向传送控制信息的第一传送方式，或设立用于在设备之间双向传送控制信息的第二传送方式，两个设备相互认证有效性，认证结果有效则共享密钥数据，使用该密匙数据来用任一设备加密控制信息，其在已设立的传送方式下被传送到另一设备。 第一设备如果已接收到控制信息，则使用对称密钥数据解密控制信息来用于解密内容数据。



1. 一种传送处理方法，用于从一个设备向另一个设备传送，除了用于加密内容数据的解密的密钥数据之外，还传送包括用于使用所述内容数据的条件的需要的信息，所述传送处理方法包含：

在所述两个设备之间进行有效性的相互认证；

用具有在所述认证期间获得的对称密钥数据的所述两个设备中的一个加密所述需要的信息；

选择提供以在所述两个设备两者之间进行数据传送的多个预定处理方式中的一个；以及

根据所述选择的传送处理方式，将已用所述两个设备中的一个加密的所述需要的信息传送到另一个设备。

2. 根据权利要求 1 所述的方法，其中：

所述多个传送处理方式包括：第一传送方式，用于从所述两个设备中的一个向另一个设备单向传送所述需要的信息；以及第二传送方式，用于在所述两个设备之间双向传送所述需要的信息；并且

已接收到根据任何一个选择的传送方式传送的所述需要的信息的所述设备，用所述对称密钥数据解密所述需要的信息，并且用所述解密的需要的信息解密所述获取的内容数据。

3. 一种传送处理方法，用于从一个设备向另一个设备传送，除了用于加密内容数据的解密的密钥数据之外，还传送包括用于使用所述内容数据的条件的需要的信息，所述传送处理方法包含：

对通过以控制所述两个设备之间的数据传送的处理装置行使控制；

向所述两个设备查询关于用于所述设备的各自内部数据的传送功能；

作为所述查询的结果，在所述两个设备之间的所述数据传送之前，选择或者第一传送方式或者第二传送方式中的一个，所述第一传送方

式用于从所述两个设备中的一个向另一个设备单向传送所述需要的信息，所述第二传送方式用于在所述两个设备之间双向传送所述需要的信息；

在所述两个设备之间进行有效性的相互认证，并且如果认证结果指示有效，则在所述两个设备之间共享密钥数据；

通过使用所述共享的密钥数据，用所述两个设备中的一个加密所述需要的信息；以及

以所述选择的传送处理方式，将已用所述两个设备中的一个加密的所述需要的信息传送到另一个设备。

4. 根据权利要求 3 所述的方法，其中：

在所述需要的信息的所述传送期间，所述两个设备两者都生成与所述需要的信息的处理相关的事项记录并将所述事项记录存储到存储装置中；并且

如果在所述有效性认证期间丢失所述密钥数据，则所述两个设备中的每一个查阅所述存储装置之内存储的所述适当事项记录，然后生成将要共享的密钥数据，并且将所述共享的密钥数据发送到另一个设备。

5. 根据权利要求 4 所述的方法，其中：

另一个设备查阅所述存储装置之内存储的所述事项记录，连接所述事项记录中记录的处理阶段信息和有关所述需要的信息的存在状态信息，并且传输所述连接的两组信息；并且

在检验接收的信息并确认没有进行伪造之后，所述两个设备中的一个查阅所述存储装置之内存储的所述适当事项记录，并且用所述事项记录中记录的先前传送数据的解密使能条件重写所述现存的需要的信息。

6. 根据权利要求 2 至 5 中任何一项所述的方法，其中：

如果选择了所述第二传送方式，则在所述有效性认证期间：

另一个设备向所述两个设备中的一个传输包括所述设备的固有公共密钥的证书；

所述两个设备中的一个检验所述接收的证书的有效性，生成第一质询密钥，其为用于临时对称密钥加密的密钥，用所述接收的公共密钥加密所述第一质询密钥，将包括所述设备的固有公共密钥的证书连接到生成的所述加密的数据，并且传输所述连接的两组数据；

另一个设备通过用所述设备的固有私有密钥解密所述接收的数据来获取所述第一质询密钥，生成第二质询密钥，其为用于临时对称密钥加密的密钥，连接所述第二质询密钥和所述设备的固有信息区域中嵌入的公共密钥，用所述接收的公共密钥进行加密，将所述设备的固有证书撤销清单连接到已获得的所述加密的数据，用所述第一质询密钥加密所述连接的两组数据，并且向所述两个设备中的一个传输所述加密的数据；

所述两个设备中的一个用所述第一质询密钥解密所述接收的数据，将所述证书撤销清单中包含的清单发布日期信息与分配给所述设备的固有证书撤销清单的确认日期信息相比较，因此，如果另一个设备的所述接收的证书撤销清单的所述发布日期是较新的，则将另一个设备的所述证书撤销清单更新为所述设备的固有清单；

另外，所述两个设备中的一个用所述设备的固有私有密钥解密除了所述证书撤销清单之外的全部加密数据， 进一步生成第零阶第一会话密钥，其为用于临时对称密钥加密的密钥，用所述以前接收的公共密钥和另一个设备的第二质询密钥进行加密，并且向另一个设备传输所述加密的数据；以及

另一个设备解密接收的所述加密数据，然后如果所述解密的数据包括所述两个设备中的一个的所述证书撤销清单，则通过使用所述接收的证书撤销清单更新所述设备的固有证书撤销清单，并且通过用所述设备的固有信息区域中嵌入的所述私有密钥解密除了所述证书撤销清单之外的全部所述加密数据，来获取所述第零阶第一会话密钥。

7. 根据权利要求 2 至 6 中任何一项所述的方法，其中：

如果选择了所述第二传送方式，则在所述需要的信息的传送处理期间：

另一个设备生成第 n 阶第二会话密钥，通过使用以前生成的第 n－1阶第二会话密钥和当时最新的第m阶第一会话密钥来加密所述第n阶第二会话密钥，并且将所述加密的数据传输到所述两个设备中的一个；

所述两个设备中的一个在接收到所述加密数据之后，通过使用所述当时最新的第m阶第一会话密钥和所述第n－1阶第二会话密钥来解密所述数据，并且在所述事项记录中记录将要传送的所述需要的信息的标识符、所述设备在传送中的固有角色、计划传输的所述需要的信息以及另一个设备中的所述需要的信息的记录目标地址；

另外，所述两个设备中的一个向所述需要的信息连接指示其使用目的（亦即至少包括或复制、移动或再现/回放的目的）的参数和校验和，用所述第 n 阶第二会话密钥和所述共享密钥进行加密，并且将所述加密的数据传输到另一个设备；以及

另一个设备在接收到所述加密数据之后，通过使用所述共享的密钥和所述第 n 阶第二会话密钥来解密所述数据，并且在另一个设备的内部存储区域中记录所述解密的数据。

8. 根据权利要求 1 至 7 中任何一项所述的方法，其中：

所述需要的信息是许可信息，其包括用于允许内容数据被解密的条件；并且

另一个设备在接收到所述许可信息之后，使用所述许可信息以解密从所述两个设备中的一个传输的并且存储在所述存储装置之内的所述内容数据。

9. 根据权利要求 1 至 8 中任何一项所述的方法，其中：

所述两个设备中的一个是记录器/播放器，其具有分别用于记录和再现获取的内容数据的记录模块和回放模块，另一个设备是存储装置，其连接到所述记录器/播放器并适合于存储从其中传送的所述内容数

据，当所述记录器/播放器获取所述内容数据时获取所述需要的信息，并且已被记录在所述存储装置中的所述内容数据被从其中传送到所述记录器/播放器，然后由所述回放模块再现。

10. 一种处理方法，用于处理除了用于对加密的内容数据进行解密的密钥数据之外，还处理包括用于使用所述内容数据的条件的需要的信息，并且从一个设备向另一个设备既传送所述密钥数据又传送所述需要的信息，所述处理方法包含：

（a）认证步骤，用于在所述两个设备之间进行有效性的相互认证，并且如果认证结果指示两个设备都有效，则在其间共享所述密钥数据；以及

（b）传送步骤，用于用具有所述共享的密钥数据的所述两个设备中的一个加密所述需要的信息，并且从一个设备向另一个设备传送所述加密的需要的信息；

其中：

在认证步骤（a）中，

另一个设备传输包括所述设备的固有公共密钥的证书，

所述两个设备中的一个检验所述接收的证书的有效性，生成第一质询密钥，其为用于临时对称密钥加密的密钥，用所述接收的公共密钥加密所述第一质询密钥，将包括所述设备的固有公共密钥的证书连接到生成的所述加密数据，并且将所述连接的两组数据传输到另一个设备，

另一个设备通过用所述设备的固有私有密钥解密所述接收的数据来获取所述第一质询密钥，生成第二质询密钥，其为用于临时对称密钥加密的密钥，连接所述第二质询密钥和所述设备的固有信息区域中嵌入的公共密钥，用所述接收的公共密钥进行加密，将所述设备的固有证书撤销清单连接到已获得的所述加密数据，用所述第一质询密钥加密所述连接的两组数据，并且将所述加密数据传输到所述两个设备中的一个，

所述两个设备中的一个用所述第一质询密钥解密所述接收的数

据，将所述证书撤销清单中包含的清单发布日期信息与分配给所述设备的固有证书撤销清单的确认日期信息相比较，因此，如果另一个设备的所述接收的证书撤销清单的所述发布日期是较新的，则将另一个设备的所述证书撤销清单更新为所述设备的固有清单，

另外，所述两个设备中的一个用所述设备的固有私有密钥解密除了所述证书撤销清单之外的全部加密数据， 进一步生成第零阶第一会话密钥，其为用于临时对称密钥加密的密钥，用所述以前接收的公共密钥和另一个设备的第二质询密钥进行加密，并且向另一个设备传输所述加密的数据；以及

另一个设备解密接收的所述加密数据，然后如果所述解密的数据包括所述两个设备中的一个的所述证书撤销清单，则通过使用所述接收的证书撤销清单更新所述设备的固有证书撤销清单，并且通过用所述设备的固有信息区域中嵌入的所述私有密钥解密除了所述证书撤销清单之外的全部所述加密数据，来获取所述第零阶第一会话密钥；并且

在传送步骤（b）中，

另一个设备生成第 n 阶第二会话密钥，通过使用以前生成的第 n－1阶第二会话密钥和当时最新的第m阶第一会话密钥来加密所述第n阶第二会话密钥，并且将所述加密的数据传输到所述两个设备中的一个，

所述两个设备中的一个在接收到所述加密数据之后，通过使用当时最新的第m阶第一会话密钥和所述第n－1阶第二会话密钥来解密所述数据，并且在所述事项记录中记录将要传送的所述需要的信息的标识符、所述设备在传送中的固有角色、计划传输的所述需要的信息以及另一个设备中的所述需要的信息的记录目标地址，

另外，所述两个设备中的一个向所述需要的信息连接指示其使用目的（亦即至少包括或复制、移动或再现/回放的目的）的参数和校验和，用所述第 n 阶第二会话密钥和所述共享密钥进行加密，并且将所述加密的数据传输到另一个设备，以及

另一个设备在接收到所述加密数据之后，通过使用所述共享的密

钥和所述第 n 阶第二会话密钥来解密所述数据，并且在另一个设备的内部存储区域中记录所述解密的数据。

11. 根据权利要求 1 至 10 中任何一项所述的方法，其中所述需要的信息包括：

格式，其指示所述信息自身能够被输出到哪种模块；

标识符，其被唯一地分配给所述特殊信息；

条件，用于限定所述内容数据使用；

密钥数据，用于解密加密的内容数据；

标识符，用于识别相关的内容数据；以及

有关内容的版权信息。

12. 一种用于以根据权利要求 1 至 11 中任何一项所述的方法执行计算机处理的程序。

13. 一种传送系统，包含：第一设备，用于记录/再现获取的内容数据；第二设备，用于存储所述内容数据；以及主机，其控制所述第一和第二设备两者之间的数据传送，并且传送打算控制所述内容数据的解密需要的信息，所述系统包含：

这样的装置，其在所述主机的控制下，向所述第一和第二设备查询关于用于所述设备的各自内部数据的传送功能；

这样的装置，其作为所述查询的结果，在所述第一和第二设备之间的所述数据传送之前，选择第一传送方式或者第二传送方式的装置，所述第一传送方式用于从所述第一设备向所述第二设备单向传送所述需要的信息，所述第二传送方式用于在所述第一和第二设备两者之间双向传送所述需要的信息；

这样的装置，其在所述第一和第二设备两者之间进行有效性的相互认证，并且如果认证结果指示有效，则在所述第一和第二设备两者之间共享密钥数据；

这样的装置，其通过使用所述共享的密钥数据，用所述两个设备

中的一个加密所述需要的信息；以及

这样的装置，其以所述选择的传送方式，将已用所述两个设备中的一个加密的所述需要的信息传送到另一个设备。

用于传送数据的方法和系统

技术领域

【0001】

本发明一般涉及用于传送数据的方法和系统。更加具体地，本发明涉及用于在记录器之间或者从存储装置向记录器/播放器传送信息的协议，所述信息打算控制加密内容数据的使用。本发明还涉及处理所述协议的包括记录器/播放器和存储装置的系统。

背景技术

【0002】

当诸如音乐数据或图像数据之类的内容数据具有版权时，存在版权持有者的权利被侵犯的风险，除非采取用于版权保护的适当措施。然而，如果应予最优先考虑的事被赋予版权保护并且内容数据的流通被阻止，则这将证明对版权持有者是不利的，所述版权持有者能够对版权所有的内容的复制品收版税。

【0003】

需要保护其版权的数据主要经由数字通信网络、广播电波等递送。当用户使用这样的数据时，用户通常在用再现装置开始再现之前将数据记录到某种存储介质上。当前，磁盘驱动器作为大容量和高存取性能的以控制为特征的存储装置是已知的。大部分的磁盘驱动器被固定地内置到记录器/播放器中，并且这样的磁盘驱动器是未知的：允许内部数据用在其他再现装置中。然而，根据操作的便利性，便携式存储装置的使用很可能在将来增长。在这样的环境下，存储卡作为便携式存储装置是已知的，其尽管在容量方面低于磁盘驱动器，但是具有版权保护功能。

【0004】

使用用于接收递送数据的记录器/播放器或用于再现的便携式专

用装置再现这样的数据。

为了保护可连接到记录器/播放器的便携式存储装置中记录的数据的版权，重要的是，既向记录器/播放器又向存储装置提供某种安全措施，以便防止记录的数据被再现超过版权持有者坚决主张的条件的范围。向装置提供安全保护需要的是，对于从装置的内外可自由存取的区域中的数据交换，应当通过例如在将要交换数据的装置之间实施认证过程，或者加密数据自身，来防止明文中的自由数据存取。然而，与此同时，随着这些认证或加密过程变得更加苛刻，从用户发出数据使用请求时直到实际上已使数据对用户可用为止所需的过程会增加，并且很可能导致不能流畅地再现数据的情形。

【0005】

例如专利参考文献 1 和 2 提议了这样的技术，在所述技术中，通过加密数据，并且与此同时，防止用于解密加密数据的密钥的以及加密数据的使用条款和条件的未被授权的获取、伪造等，来保护与将要使用的数字数据相关的版权。同样，专利参考文献 3 披露了涉及存储装置的技术，其中，从主设备发送的多个加密和输入/输出过程会被分成多个过程然后并行执行，以便当以加密的形式输入输出数据时，将在存储装置和主设备之间保密的数据的抗干扰性会改善。

【0006】

【专利参考文献 1】WO01/013358

【专利参考文献 2】WO01/043339

【专利参考文献 3】日本专利公开号 2004－302701

发明内容

【本发明要解决的问题】

【0007】

当用于解密数字数据的密钥以及加密数据的使用条款和条件将要在两个设备之间传送时，上述传统技术中披露的方法需要处理负荷高的公共密钥的加密和解密计算以及公共密钥的证书验证。然而，已发

现的是，专利参考文献 1 和 2 中披露的技术具有下述几个问题。

【0008】

首先，传送目标设备是否认证传送源设备的正确性未被考虑，因此，如果从未被授权的设备向传送目标传输密钥和使用条款与条件，则不能防止未被授权的访问，因为密钥和使用条款与条件会被记录。

第二，多个密钥和使用条款与条件要被连续传输的情形未被适当考虑，因此，每次传输密钥和使用条款与条件时，都必须在传送源设备和传送目标设备两者之间进行涉及高负荷的公共密钥加密计算。

【0009】

第三，当各个证书鉴别设备的有效性时，尽管在整个系统中和那些设备证书一起使用已撤销证书的清单，但是上述方法仅允许更新传送目标的证书撤销清单。

第四，当在两个设备之间传送密钥和使用条款与条件时，密钥和使用条款与条件的认证过程和传送方向是固定的，并且为了进行相反的传送，认证过程必须也处于相反的方向，并且从头重新开始。这向记录器/播放器和存储装置两者施加了大的负荷。

【0010】

本发明的目标是提供解决如上所述那样的问题的数据传送方法、程序和系统。

【解决问题的方法】

【0011】

根据本发明的传送处理方法，其打算从一个设备向另一个设备，除了用于加密内容数据的解密的密钥数据之外，还传送包括用于使用所述内容数据的条件的需要的信息，包括：在所述两个设备之间进行有效性的相互认证；用具有在所述认证期间获得的对称密钥数据的所述两个设备中的一个加密所述需要的信息；选择用于在所述两个设备两者之间传送的多个预定处理方式中的一个；以及根据所述选择的传

送处理方式，将已用所述两个设备中的一个加密的所述需要的信息到另一个设备。

在优选的例子中，所述多个传送处理方式包括：第一传送方式，用于从所述两个设备中的一个向另一个设备单向传送所述需要的信息；以及第二传送方式，用于在所述两个设备之间双向传送所述需要的信息；并且已接收到根据任何一个选择的传送方式传送的所述需要的信息的所述设备，用所述对称密钥数据解密所述需要的信息，并且用所述解密的信息解密所述获取的内容数据。

在另一个优选的例子中，用于从一个设备向另一个设备，除了用于加密内容数据的解密的密钥数据之外，还传送包括用于使用所述内容数据的条件的需要的信息的传送处理方法，被修改以包括：对通过以控制所述两个设备之间的数据传送的处理装置行使控制；向所述两个设备查询关于用于所述设备的各自内部数据的传送功能；作为所述查询的结果，在所述两个设备之间的所述数据传送之前，选择第一传送方式或者第二传送方式，该第一传送方式用于从所述两个设备中的一个向另一个设备单向传送所述需要的信息，该第二传送方式用于在所述两个设备之间双向传送所述需要的信息；在所述两个设备之间进行有效性的相互认证，并且如果认证结果指示有效，则在所述两个设备之间共享密钥数据；通过使用所述共享的密钥数据，用所述两个设备中的一个加密所述需要的信息；以及以所述选择的传送处理方式，将已用所述两个设备中的一个加密的所述需要的信息传送到另一个设备。

在还有另一个优选的例子中，在所述需要的信息的所述传送期间，所述两个设备两者都生成与所述需要的信息的处理相关的事项记录并将所述事项记录存储到存储装置中，并且如果在所述有效性认证期间丢失所述密钥数据，则所述两个设备中的每一个查阅所述存储装置之内存储的所述适当事项记录，然后生成将要共享的密钥数据，并且将

所述共享的密钥数据发送到另一个设备。

在仍然另一个优选的例子中，另一个设备查阅所述存储装置之内存储的所述事项记录，连接所述事项记录中记录的处理阶段信息和有关所述需要的信息的存在状态信息，并且传输所述连接的两组信息。另外，在检验接收的信息并确认没有进行伪造之后，所述两个设备中的一个查阅所述存储装置之内存储的所述适当事项记录，并且用所述事项记录中记录的先前传送数据的解密使能条件重写所述现存的需要的信息。

在进一步优选的例子中，如果选择了所述第二传送方式，则在所述有效性认证期间：另一个设备向所述两个设备中的一个传输包括所述设备的固有公共密钥的证书；所述两个设备中的一个检验所述接收的证书的有效性，生成第一质询密钥(challenge key)，其为用于临时对称密钥加密的密钥，用所述接收的公共密钥加密所述第一质询密钥，将包括所述设备的固有公共密钥的证书连接到生成的所述加密的数据，并且传输所述连接的两组数据；另一个设备通过用所述设备的固有私有密钥解密所述接收的数据来获取所述第一质询密钥，生成第二质询密钥，其为用于临时对称密钥加密的密钥，连接所述第二质询密钥和所述设备的固有信息区域中嵌入的公共密钥，用所述接收的公共密钥进行加密，将所述设备的固有证书撤销清单连接到已获得的所述加密的数据，用所述第一质询密钥加密所述连接的两组数据，并且向所述两个设备中的一个传输所述加密的数据；所述两个设备中的一个用所述第一质询密钥解密所述接收的数据，将所述证书撤销清单中包含的清单发布日期信息与分配给所述设备的固有证书撤销清单的确认日期信息相比较，因此，如果另一个设备的所述接收的证书撤销清单的所述发布日期更新，则将另一个设备的所述证书撤销清单更新为所述设备的固有清单；另外，所述两个设备中的一个用所述设备的固有私有密钥解密除了所述证书撤销清单之外的全部加密数据， 进一步生成第零阶第一会话密钥，其为用于临时对称密钥加密的密钥，用所述

以前接收的公共密钥和另一个设备的第二质询密钥进行加密，并且向另一个设备传输所述加密的数据；以及另一个设备通过使用所述第二质询密钥解密接收的所述加密数据，然后如果所述解密的数据包括所述两个设备中的一个的所述证书撤销清单，则通过使用所述接收的证书撤销清单更新所述设备的固有证书撤销清单，并且通过用所述设备的固有信息区域中嵌入的所述私有密钥解密除了所述证书撤销清单之外的全部所述加密数据，来获取所述第零阶第一会话密钥。

在进一步优选的例子中，如果选择了所述第二传送方式，则在所述需要的信息的传送处理期间：另一个设备生成第 n 阶第二会话密钥，通过使用以前生成的第 n－1 阶第二会话密钥和当时最新的第 m 阶第一会话密钥来加密所述第 n 阶第二会话密钥，并且将所述加密的数据传输到所述两个设备中的一个；所述两个设备中的一个在接收到所述加密数据之后，通过使用所述当时最新的第 m 阶第一会话密钥和所述第 n－1 阶第二会话密钥来解密所述数据，并且在所述事项记录中记录将要传送的所述需要的信息的标识符、所述设备在传送中的固有角色、计划传输的所述需要的信息以及另一个设备中的所述需要的信息的记录目标地址；另外，所述两个设备中的一个向所述需要的信息连接指示其使用目的（亦即至少包括或复制、移动或再现/回放的目的）的参数和校验和，用所述第 n 阶第二会话密钥和所述共享密钥进行加密，并且将所述加密的数据传输到另一个设备；以及另一个设备，在接收到所述加密数据之后，通过使用所述共享的密钥和所述第 n 阶第二会话密钥来解密所述数据，并且在另一个设备的内部存储区域中记录所述解密的数据。

另外，优选地，所述需要的信息是许可信息，其包括用于允许内容数据被解密的条件，并且另一个设备在接收到所述许可信息之后，使用所述许可信息以解密从所述两个设备中的一个传输的并且存储在所述存储装置之内的所述内容数据。

进而，优选地，所述两个设备中的一个是记录器/播放器，其具有分别用于记录和再现获取的内容数据的记录模块和回放模块，另一个设备是存储装置，其连接到所述记录器/播放器并适合于存储从其中传送的所述内容数据，当所述记录器/播放器获取所述内容数据时获取所述需要的信息，并且已被记录在所述存储装置中的所述内容数据被从其中传送到所述记录器/播放器，然后由所述回放模块再现。

【0012】

另外，本发明提议了以下传送方法作为其特有的传送方法中的一个。亦即，一种处理方法，用于除了用于加密内容数据的解密的密钥数据之外，还处理包括用于使用所述内容数据的条件的需要的信息，并且从一个设备向另一个设备既传送所述密钥数据又传送所述需要的信息，所述处理方法包含：（a）认证步骤，用于在所述两个设备之间进行有效性的相互认证，并且如果认证结果指示两个设备都有效，则在其间共享所述密钥数据；以及（b）传送步骤，用于用具有所述共享的密钥数据的所述两个设备中的一个加密所述需要的信息，并且从一个设备向另一个设备传送所述加密的需要的信息。

在认证步骤（a）中：

另一个设备传输包括所述设备的固有公共密钥的证书，所述两个设备中的一个检验所述接收的证书的有效性，生成第一质询密钥，其为用于临时对称密钥加密的密钥，用所述接收的公共密钥加密所述第一质询密钥，将包括所述设备的固有公共密钥的证书连接到生成的所述加密数据，并且传输所述连接的两组数据，

另一个设备通过用所述设备的固有私有密钥解密所述接收的数据来获取所述第一质询密钥，生成第二质询密钥，其为用于临时对称密钥加密的密钥，连接所述第二质询密钥和所述设备的固有信息区域中嵌入的公共密钥，用所述接收的公共密钥进行加密，将所述设备的固有证书撤销清单连接到已获得的所述加密数据，用所述第一质询密钥加密所述连接的两组数据，并且将所述加密数据传输到所述两个设备中的一个，

所述两个设备中的一个用所述第一质询密钥解密所述接收的数据，将所述证书撤销清单中包含的清单发布日期信息与分配给所述设备的固有证书撤销清单的确认日期信息相比较，因此，如果另一个设备的所述接收的证书撤销清单的所述发布日期更近，则将另一个设备的所述证书撤销清单更新为所述设备的固有清单，

另外，所述两个设备中的一个用所述设备的固有私有密钥解密除了所述证书撤销清单之外的全部加密数据， 进一步生成第零阶第一会话密钥，其为用于临时对称密钥加密的密钥，用所述以前接收的公共密钥和另一个设备的第二质询密钥进行加密，并且向另一个设备传输所述加密的数据；以及

另一个设备解密接收的所述加密数据，然后如果所述解密的数据包括所述两个设备中的一个的所述证书撤销清单，则通过使用所述接收的证书撤销清单更新所述设备的固有证书撤销清单，并且通过用所述设备的固有信息区域中嵌入的所述私有密钥解密除了所述证书撤销清单之外的全部所述加密数据，来获取所述第零阶第一会话密钥。

在传送步骤（b）中：

另一个设备生成第 n 阶第二会话密钥，通过使用以前生成的第 n－1阶第二会话密钥和当时最新的第m阶第一会话密钥来加密所述第n阶第二会话密钥，并且将所述加密的数据传输到所述两个设备中的一个，

所述两个设备中的一个在接收到所述加密数据之后，通过使用当时最新的第m阶第一会话密钥和所述第n－1阶第二会话密钥来解密所述数据，并且在所述事项记录中记录将要传送的所述需要的信息的标识符、所述设备在传送中的固有角色、计划传输的所述需要的信息以及另一个设备中的所述需要的信息的记录目标地址，

另外，所述两个设备中的一个向所述需要的信息连接指示其使用目的（亦即至少包括或复制、移动或再现/回放的目的）的参数和校验和，用所述第 n 阶第二会话密钥和所述共享密钥进行加密，并且将所述加密的数据传输到另一个设备，以及

另一个设备在接收到所述加密数据之后，通过使用所述共享的密钥和所述第 n 阶第二会话密钥来解密所述数据，并且在另一个设备的内部存储区域中记录所述解密的数据。

在进一步的例子中，所述需要的信息包括：格式，其指示所述信息自身能够被输出到哪种模块；标识符，其被唯一地分配给所述特殊信息；条件，用于限定所述内容数据使用；密钥数据，用于解密加密的内容数据；标识符，用于识别相关的内容数据；以及有关内容的版权信息。

进而，本发明能够被理解为打算以上述方法中的任何一种执行计算机处理的程序。

此外，本发明能够被理解为设计用来以上述方法中的任何一种执行处理的系统。

【本发明的效果】

【0013】

根据本发明，可以提供当从一个设备向另一个设备，不仅传送用于解密多组数据的密钥，而且还传送有关每组数据的包括使用条件的控制信息时，减少多个设备的加密计算上的负荷的适当方法。

同样，能够在有效设备之间安全地传送控制信息。向无效设备传送控制信息被传送源设备拒绝，并且即使从无效设备传送控制信息，传送目标设备也能够拒绝接收信息。

另外，在从一个设备向另一个设备传送控制信息的系统中，如果传送目标设备具有的撤销证书清单比传送源设备具有的清单新，则传送源设备的清单能够用于更新传送目标设备的清单，同时在设备之间进行相互认证过程。

附图说明

图 1 是显示包括本发明的实施例应用于其的记录器/播放器的数据保护系统的示意性配置图。

图 2 是根据上述实施例的可移动磁盘驱动器的配置图。

图 3 是列举实施例中使用的数据、信息、编码/解码方案等的表格。

图 4 是列举对实施例中使用的数据的解密条件和解密密钥的数据（使用通行证）结构图。

图 5 是显示在实施例中的图 2 的磁盘驱动器中实现 UT 方式的使用通行证传送模块 530 的示图。

图 6 是显示在根据实施例的记录器/播放器中实现 UT 方式的只记录功能模块的示图。

图 7 是显示在根据实施例的记录器/播放器中实现 UT 方式的只解密功能模块的示图。

图 8 是显示用于记录根据实施例的记录器/播放器中在 UT 方式下使用的证书、公共密钥、私有密钥、使用通行证传送处理记录信息以及其他私有信息的抗干扰静态存储区域的示图。

图 9 是显示用于记录根据实施例的磁盘驱动器中在 UT 方式下使用的证书、公共密钥、私有密钥、使用通行证传送处理记录信息以及其他私有信息的抗干扰静态存储区域的示图。

图 10 是显示用于记录根据实施例的磁盘驱动器中的使用通行证的抗干扰静态存储区域的示图。

图 11 是显示在磁盘驱动器中实现 BT 方式的功能模块的示图。

图 12 是显示在记录器/播放器中实现 BT 方式下的使用通行证传输的只记录功能模块的示图。

图 13 是显示在记录器/播放器中实现 BT 方式下的使用通行证传输的只解密功能模块的示图。

图 14 是显示关于记录器/播放器中的 BT 方式下的磁盘驱动器实现相互认证的只解密功能模块的示图。

图 15 是显示用于记录磁盘驱动器中在 BT 方式下使用的证书、公

共密钥、私有密钥、相互认证处理记录信息、使用通行证传送处理记录信息以及其他私有信息的抗干扰静态存储区域的示图。

图 16 是显示用于记录磁盘驱动器中在 UT 方式下使用的证书、公共密钥、私有密钥、相互认证处理记录信息、使用通行证传送处理记录信息以及其他私有信息的抗干扰静态存储区域的示图。

图 17 是显示用于实施例中的使用通行证传送处理期间的访问方式识别和设立的处理顺序的示图。

图 18 是显示实施例中的 UT 方式下的记录器/播放器和存储装置之间进行的相互认证处理顺序的示图。

图 19 是显示实施例中的 UT 方式下的记录器/播放器和磁盘驱动器之间进行的使用通行证传送处理顺序的示图。

图 20 是显示实施例中的 UT 方式下的记录器/播放器和磁盘驱动器之间进行的简化相互再认证处理顺序的示图。

图 21 是显示实施例中的为了恢复丢失的使用通行证的 UT 方式下的记录器/播放器和磁盘驱动器之间进行的处理顺序的示图。

图 22 是显示实施例中的 BT 方式下的记录器/播放器和磁盘驱动器之间进行的相互认证处理顺序的示图。

图 23 是显示实施例中的 BT 方式下的从记录器/播放器到磁盘驱动器的使用通行证传输的传送处理顺序的示图。

图 24 是显示实施例中的 BT 方式下的从磁盘驱动器到记录器/播放器的使用通行证传输的传送处理顺序的示图。

图 25 是显示实施例中的 BT 方式下的记录器/播放器和磁盘驱动器之间进行的简化相互再认证处理顺序的示图。

图 26 是显示在实施例中的 BT 方式下进行的处理顺序的示图，目的是为了恢复已在从记录器/播放器向磁盘驱动器传输之后丢失的使用通行证。

图 27 是显示在实施例中的 BT 方式下进行的处理顺序的示图，目的是为了恢复已在从磁盘驱动器向记录器/播放器传输之后丢失的使用通行证。

图 28 是显示实施例中的主机模块和设备 2 之间的指令传送顺序的

示图。

具体实施方式

【0014】

在下文中将说明本发明的优选实施例。

下面的说明预先假定：需要保护的数据被加密；解密数据所需的密钥数据和允许解密的条件被集成到一组数据中；并且该组数据存储在从用户不可自由访问的存储区域中。由密钥数据和允许解密的条件组成的相互关联的一组数据将在下面的实施例中被称作使用通行证(Usage Pass)。

本发明披露了应用于从一个模块向另一个模块传送使用通行证的各种过程和处理序列。存在两种处理序列。它们中的一种是 UT（单向传送）方式，其中使用通行证的传送方向被唯一确定，而另一种则是 BT（双向传送）方式，其中能够双向传送使用通行证。以下作为优选实施例说明用于在例如记录器/播放器和存储装置的两个设备之间传送的这些截然不同的使用通行证的传送方法的应用。

【0015】

在记录器/播放器和存储装置之间使用通行证的传送之前，依据两种方式中的哪一种将要用于执行使用通行证传送，首先选择记录器/播放器的适当内部处理器（在下面的实施例中为主机模块）。然后将相关方式通知给将要发送或接收使用通行证的两个设备的各个模块。下面首先来说明对使用通行证发送或接收模块设置 UT 方式的情况下的传送。

【0016】

当设置 UT 方式时，将要最终接收使用通行证的模块向将要发送使用通行证的模块传输该模块的数据中嵌入的设备类别证书。设备类别证书包括设备类别公共密钥。在 UT 方式下，包括使用通行证发送模块的设备会被称作“原始设备(Primal Device)”，而包括接收模块的设

备则会被称作“开始设备(Inceptive Device)”。在这个意义下，设备类别证书会被称作“开始设备类别证书”，而设备类别公共密钥则会被称作“开始设备类别公共密钥”。

【0017】

原始设备检验接收的证书的有效性，并且如果检验结果指示了接收的证书的有效性，则产生原始质询密钥，其为用于临时对称密钥加密的密钥。在这之后，原始设备通过使用接收的设备类别证书加密原始质询密钥，向产生且加密的数据连接包括原始设备类别公共密钥的原始设备类别证书，并且将连接的数据和证书发送到开始设备。

【0018】

开始设备通过使用它的固有设备类别私有密钥来解密接收的数据，并且获取原始质询密钥。下一步，开始设备产生第零阶开始会话密钥，其为用于临时对称密钥加密的密钥。在产生这个密钥之后，开始设备将该密钥连接到设备的固有数据中嵌入的开始设备类别公共密钥，并且用接收的原始设备类别密钥进行加密。另外，开始设备向如此获得的数据连接设备自身中记录的撤销设备类别清单(开始 RDCL)，并且用接收的原始质询密钥进行加密。在进行上述过程步骤之后，开始设备将获得的数据发送到原始设备。

【0019】

然后原始设备使用原始质询密钥解密接收的数据，并且从解密结果中取出开始 RDCL。由于 RDCL 包括数据的发布日期信息，所以原始设备将开始 RDCL 的发布日期信息与设备自身中记录的 RDCL（原始 RDCL）的发布日期信息相比较。结果，如果开始 RDCL 的发布日期更新，则用开始 RDCL 重写原始 RDCL。在比较 RDCL 发布日期之后，原始设备使用原始设备私有密钥解密剩余的数据。下一步，原始设备产生第零阶原始会话密钥，其为用于临时对称密钥加密的密钥。在产生这个密钥之后，原始设备用以前接收的第零阶开始会话密钥进行加密。此时，如果以前的对 RDCL 发布日期信息的比较指示原始 RDCL 的发布日期更新，则原始设备将原始 RDCL 连接到以前加密的数据。下一步，原始设备用以前接收的开始设备公共密钥加密获得的

数据。在加密之后，原始设备将获得的数据发送到开始设备。

【0020】

然后开始设备使用开始设备私有密钥解密接收的数据。如果解密结果包括原始 RDCL，则开始设备用原始 RDCL 重写开始 RDCL。下一步，开始设备通过使用第零阶开始会话密钥来解密剩余的数据，并且这样一来就获得了第零阶原始会话密钥。

上面是 UT 方式下的认证过程。这个过程被称作“UT 连接阶段”。第零阶原始会话密钥、第零阶开始会话密钥以及在用开始设备公共密钥加密和用开始设备私有密钥解密期间获得的对称开始设备密钥，在 UT 连接阶段完成之后被共享。

【0021】

在认证之后，能够执行使用通行证传送。以下述序列进行 UT 方式下的使用通行证的传送。仅在从原始设备向开始设备的方向上进行 UT 方式下的使用通行证传送。

首先，原始设备在使用通行证传送模块中设立预期使用通行证。下一步，主机模块向开始设备发送 UPID，即用于识别预期使用通行证的标识符。

【0022】

开始设备产生用于加密使用通行证的第 n 阶开始会话密钥，并且将开始会话密钥和 UPID 一起记录在被称作“开始事项记录”的记录中。传送过程阶段（RP）也记录在这个记录中。该记录用于恢复使用通行证的初始状态，如果使用通行证传送过程获致异常终止的话。在产生第 n 阶开始会话密钥之后，开始设备用以前的使用通行证传送期间产生的开始会话密钥（第 n－1 阶开始会话密钥）和第零阶原始会话密钥进行加密，并且将加密结果传输到原始设备。

【0023】

原始设备通过使用第零阶原始会话密钥和第 n－1 阶开始会话密钥来解密接收的数据。在那之后，原始设备在原始设备记录中记录以

下数据：将要传送的使用通行证的 UPID；开始设备类别证书中包含的参数数据的部分；在连接阶段期间接收的开始设备公共密钥；从上述解密结果中获得的第 n 阶开始会话密钥；传送过程阶段（SP）；将要传送的使用通行证中包括的数据的解密使能条件；以及已记录使用通行证的地址。

下一步在从使用通行证发送模块中设立的使用通行证中产生将要实际传输的使用通行证之后，原始设备将指示使用目的（或复制、移动或再现/回放）的参数和“校验和”连接到将要传输的使用通行证，并且通过使用第 n 阶开始会话密钥和对称开始设备密钥来加密数据。在加密之后，原始设备将原始事项记录之内的传送过程阶段单元更新到 SC，并且将数据传输到开始设备。

【0024】

开始设备用对称开始设备密钥和第零阶开始会话密钥解密接收的数据。下一步，开始设备将开始事项记录之内的传送过程阶段单元更新到 RC，在开始事项记录中记录使用通行证的记录目标地址，并且在使用通行证存储区域中记录数据。

上面是 UT 方式下的使用通行证传送过程。这个过程被称作“UT 传送阶段”。如上所述，UT 方式下的使用通行证传送固定在从原始设备到开始设备的方向。

【0025】

如果在使用通行证传送过程的执行期间，在记录器/播放器中发生诸如电源停止之类的异常，并且在使用通行证传送源和使用通行证传送目标两者中丢失使用通行证，则通过进行下面的过程步骤，能够恢复使用通行证的初始状态。

如果发生异常，则在 UT 连接阶段期间共享的第零阶原始会话密钥、第零阶开始会话密钥以及对称设备密钥，全部都在记录器/播放器和存储装置中丢失。因此必须重新共享这些密钥。然而，UT 连接阶段

并不需要重新执行，并且需要的全部只是执行下述处理。

【0026】

首先，主机向原始设备传输将要恢复的使用通行证的 UPID。然后原始设备使用 UPID 搜索原始事项记录。如果包括所述 UPID 的原始事项记录从而被检测到，则原始设备产生新的第零阶原始会话密钥。下一步，原始设备用检测到的原始事项记录中以前记录的会话密钥和开始设备公共密钥加密产生的会话密钥，并且将加密数据传输到开始设备。然后开始设备解密接收的数据并获得新的第零阶原始会话密钥和对称设备密钥。

上面是 UT 方式下的再认证过程。这个过程被称作“UT 再连接阶段”。新的第零阶原始会话密钥以及在用开始设备公共密钥加密和用开始设备私有密钥解密期间获得的新的对称开始设备密钥，在 UT 再连接阶段完成之后被共享。

【0027】

UT 再连接阶段的完成被继之以原始设备中的以下使用通行证恢复过程：

主机向开始设备传输将要恢复的使用通行证的 UPID。然后开始设备使用接收的 UPID 搜索开始事项记录。如果包括所述 UPID 的开始事项记录从而被检测到，则开始设备连接事项记录中记录的过程阶段信息和使用通行证的存在状态信息，然后将如此连接的数据传输到原始设备。在连接数据的传输之前，已从数据自身中计算的散列值(Hash value)、第零阶原始会话密钥以及开始事项记录中记录的开始设备会话密钥，也会进一步连接到上述数据。

【0028】

下一步，原始设备检查接收的散列值并检验接收的数据未被伪造。在检验之后，原始设备搜索包括接收的 UPID 的原始事项记录。当发现所述记录时，原始设备用现存的使用通行证重写所述记录中记录的以前传送的解密使能条件。

上面是 UT 方式下的使用通行证恢复过程。这个过程被称作“UT 恢复阶段”。当这个阶段完成时，进行上述传输过程之前存在的使用通行证会存在于原始设备中。

【0029】

下一步，下面将说明对使用通行证发送或接收模块设置 BT 方式情况下的传送。

在 BT 方式下，使用通行证的传送方向是不固定的，并且原始设备和开始设备两者都能够发送/接收使用通行证。在 BT 方式下进行相互认证过程和使用通行证发送/接收过程的记录器/播放器的内部模块被称作开始设备，而进行相互认证过程和使用通行证发送/接收过程的存储装置的内部模块则被称作原始设备。设备类别证书被称作开始设备类别证书，而设备类别公共密钥则被称作开始设备类别公共密钥。

【0030】

原始设备检验接收的证书的有效性，并且如果检验结果指示了接收的证书的有效性，则产生原始质询密钥，其为用于临时对称密钥加密的密钥。在这之后，原始设备通过使用接收的设备类别公共密钥来加密原始质询密钥，向产生并加密的数据连接包括原始设备类别公共密钥的原始设备类别证书，并且将连接的数据和证书发送到开始设备。

【0031】

开始设备通过使用它的固有设备类别私有密钥来解密接收的数据，并且这样一来就获得了原始质询密钥。

下一步，开始设备产生开始会话密钥，其为用于临时对称密钥加密的密钥。在产生这个密钥之后，开始设备将所述密钥连接到设备的固有数据中嵌入的开始设备类别公共密钥，并且用接收的原始设备类别密钥进行加密。另外，开始设备向如此获得的数据（亦即用原始设备类别密钥加密的数据）连接设备自身中记录的撤销设备类别清单（开始 RDCL），并且用接收的原始质询密钥进行加密。在进行上述过程步骤之后，开始设备将获得的数据发送到原始设备。

【0032】

然后原始设备使用原始质询密钥解密接收的数据（加密数据），并且从解密结果中取出开始 RDCL。由于 RDCL 包括数据的发布日期信息，所以原始设备比较开始 RDCL 的发布日期信息和设备自身中记录的 RDCL（原始 RDCL）的发布日期信息。结果，如果开始 RDCL 的发布日期更新，则用开始 RDCL 重写原始 RDCL。在比较 RDCL 发布日期之后，原始设备使用原始设备私有密钥解密剩余的数据。下一步，原始设备产生第零阶原始会话密钥，其为用于临时对称密钥加密的密钥。在产生这个密钥之后，原始设备用以前接收的第零阶开始会话密钥进行加密。此时，如果以前的对 RDCL 发布日期信息的比较指示原始 RDCL 的发布日期更新，则原始设备将原始 RDCL 连接到以前加密的数据。下一步，原始设备用以前接收的开始质询密钥加密获得的数据。在进行加密之后，原始设备将获得的数据发送到开始设备。

【0033】

然后开始设备使用开始质询密钥解密接收的数据。如果解密结果包括原始 RDCL，则开始设备用原始 RDCL 重写开始 RDCL。在这之后，开始设备使用原始设备公共密钥解密剩余的数据，这样一来就获得了第零阶原始会话密钥。

然后原始设备通过用原始设备私有密钥和第零阶原始会话密钥解密接收的数据来获得第零阶开始会话密钥。在这之后，原始设备在原始连接记录中记录开始设备公共密钥、第零阶开始会话密钥、第零阶原始会话密钥以及开始设备类别证书中包括的参数的部分。

上面是 BT 方式下的认证过程。这个过程被称作“BT 连接阶段”。第零阶原始会话密钥、第零阶开始会话密钥、在用原始设备公共密钥加密和用原始设备私有密钥解密期间获得的对称原始设备密钥、以及在用开始设备公共密钥加密和用开始设备私有密钥解密期间获得的对称开始设备密钥，在 BT 连接阶段完成之后被共享。

【0034】

在认证过程之后，能够执行使用通行证的传送。下面首先说明从原始设备到开始设备的使用通行证的传送。

首先，原始设备在使用通行证发送模块中设立预期使用通行证。

在这之后，开始设备产生用于加密使用通行证的第 n 阶开始会话密钥。在这个密钥产生之后，开始设备用紧接着以前的从原始设备向开始设备的使用通行证发送期间产生的开始会话密钥（第 n－1 阶开始会话密钥），并且用那个时间点的最新原始会话密钥，来进行数据加密，然后将加密的数据传输到原始设备。

【0035】

已接收到加密数据的原始设备通过使用那个时间点的最新原始会话密钥和第 n－1 阶开始会话密钥来解密数据。同样，原始设备在适当的事项记录中记录将要传送的使用通行证的 UPID、角色（原始设备自身作为传送源的传送功能）、以及计划传输的使用通行证。在 BT 方式下，只有原始设备执行事项记录中的记录。

在这之后，从已在使用通行证发送模块中设立的使用通行证中产生将要实际传输的使用通行证。下一步在事项记录中记录开始设备中的使用通行证的记录目标地址之后，原始设备将指示使用目的（复制、移动或再现/回放）的参数和“校验和”连接到使用通行证，并且通过使用第 n 阶开始会话密钥和对称开始设备密钥来加密数据。在进行加密之后，原始设备将数据传输到开始设备。

开始设备，在接收加密数据之后，通过使用对称开始设备密钥和第 n 阶开始会话密钥来解密数据，并且在开始设备内部提供的使用通行证存储区域中记录数据。

上面是 BT 方式下从原始设备向开始设备的使用通行证传送。这个过程被称作“BT PI 传送阶段”。

【0036】

下面首先说明从开始设备向原始设备的使用通行证的传送。首先，开始设备在使用通行证传送模块中设立预期使用通行证。

在这之后，开始设备用 0 替换使用通行证的加密数据密钥部分。下一步在连接使用通行证的状态信息（该数据被称作“屏蔽的使用通行证”）之后，开始设备进一步将最新的原始会话密钥和开始会话密钥连接到数据并计算散列值。开始设备将如此获得的散列值连接到屏蔽的使用通行证，并且将散列值传输到原始设备。

【0037】

原始设备检查接收的散列值并检验接收的数据未被伪造。在检验之后，原始设备在适当的事项记录中记录接收的使用通行证 UPID、数据的解密使能条件、以及开始设备中的使用通行证的记录地址。在这之后，原始设备产生第 m 阶原始会话密钥，然后用紧接着以前的从开始设备向原始设备的使用通行证发送期间产生的原始会话密钥（第 m－1 阶原始会话密钥），并且用那个时间点的最新开始会话密钥，来进行数据加密，然后将加密的数据传输到开始设备。

【0038】

已接收到加密数据的开始设备通过使用那个时间点的最新开始会话密钥和第 m－1 阶原始会话密钥来解密数据。同样，开始设备从使用通行证传输模块中设置的使用通行证中产生将要实际传输的使用通行证。下一步，开始设备将指示使用目的（复制、移动或再现/回放）的参数和“校验和”连接到将要传输的使用通行证，并且通过使用第 m 阶原始会话密钥和对称原始设备密钥来加密数据。在加密之后，开始设备将数据传输到原始设备。

原始设备，在接收到加密数据之后，通过使用对称原始设备密钥和第 m 阶原始会话密钥来解密数据。

上面是 BT 方式下从开始设备向原始设备的使用通行证传送。这

个过程被称作“BT IP 传送阶段”。

【0039】

如 UT 方式下那样，如果在记录器/播放器中发生异常，并且在使用通行证传送源和使用通行证传送目标两者中丢失使用通行证，则通过进行下述过程步骤，能够恢复使用通行证的初始状态。BT 方式下的再认证稍微不同于 UT 方式；BT PI 传送阶段或 BT IP 传送阶段不需要的已在过去被执行，并且只有 BT 连接阶段需要已完成。

如果发生异常，则在 BT 连接阶段期间共享的第零阶原始会话密钥、第零阶开始会话密钥、对称原始设备密钥以及对称开始设备密钥，全部都在记录器/播放器和存储装置中丢失。因此必须重新共享这些密钥。然而，BT 连接阶段并不需要重新执行，并且需要的全部只是执行下述处理。

【0040】

首先，原始设备重新产生第零阶原始会话密钥，并且在用原始连接记录中记录的开始会话密钥和开始设备公共密钥加密这个密钥之后，将获得的数据传输到开始设备。

【0041】

开始设备在接收到加密数据之后，通过使用开始设备私有密钥和开始连接记录中记录的开始会话密钥来解密数据。下一步在生成新的第零阶开始会话密钥并且用开始连接记录中记录的原始会话密钥和原始设备公共密钥加密这个密钥之后，开始设备在开始连接记录中通过重写记录接收的第零阶原始会话密钥和产生的第零阶开始会话密钥，并且将上述加密的数据传输到原始设备。

【0042】

原始设备在接收到加密数据之后，通过使用原始设备私有密钥和原始连接记录中记录的第零阶原始会话密钥来解密数据，并且在原始连接记录中通过重写记录重新产生的第零阶开始会话密钥和上述产生的第零阶原始会话密钥。

上面是 BT 方式下的再认证过程。这个过程被称作“BT 再连接阶段”。新的第零阶原始会话密钥、新的第零阶开始会话密钥、在用原始设备公共密钥加密和用原始设备私有密钥解密期间获得的新的对称原始设备密钥、以及在用开始设备公共密钥加密和用开始设备私有密钥解密期间获得的新的对称开始设备密钥，在 BT 再连接阶段完成之后被共享。

【0043】

在 BT 连接阶段或 BT 再连接阶段之后，如果存在其传送没有获致完成的过去的使用通行证，则在开始传送过程之前存在的使用通行证的状态能够使用下述方法恢复。首先说明 BT PI 传送阶段期间的恢复，然后说明 BT IP 传送阶段期间的恢复。

在 BT PI 传送阶段期间传送的使用通行证被恢复到执行传送过程之前存在的状态之前，主机向原始设备传输将要恢复的使用通行证的 UPID。

【0044】

然后原始设备使用接收的 UPID 搜索原始事项记录。如果包括所述 UPID 的原始事项记录从而被检测到，则原始设备向开始设备传输记录中记录的开始设备中的使用通行证的记录目标地址（亦即接收的使用通行证计划被记录的地址）。

开始设备访问用接收的地址访问的使用通行证存储区域，并且在检查使用通行证的记录状态之后，设立使用通行证状态中的结果。下一步，开始设备连接 UPID、涉及被搜索的使用通行证的解密使能条件、产生的使用通行证状态和使用通行证的记录目标地址，并且将连接的数据传输到原始设备。在连接的数据的传输之前，已从数据自身中计算的散列值、第 m 阶原始会话密钥以及开始事项记录中记录的第 n 阶开始设备会话密钥，也会进一步连接到上述数据。

【0045】

原始设备检查接收的散列值，并且检验接收的数据未被伪造而且

以前向开始设备传送的使用通行证并不存在。在检验之后，原始设备搜索包括接收的 UPID 的原始事项记录。当发现所述记录时，原始设备用使用通行证发送模块中现存的使用通行证重写所述记录中记录的以前传送的解密使能条件。

上面是 BT PI 传送阶段期间的使用通行证恢复过程。这个过程自身被称作 BT PI 恢复阶段。当这个阶段完成时，在进行上述传输过程之前存在的使用通行证将存在于原始设备中。

【0046】

首先，下面说明 BT IP 传送阶段期间的使用通行证的恢复。在 BT IP 传送阶段期间传送的使用通行证被恢复到执行传送过程之前存在的状态之前，主机模块向原始设备传输将要恢复的使用通行证的 UPID。

然后原始设备使用接收的 UPID 搜索原始事项记录。如果包括所述 UPID 的原始事项记录从而被检测到，则原始设备向开始设备传输记录中记录的开始设备中的使用通行证的记录目标地址（亦即指示初始记录计划传送的使用通行证的区域的地址）。

【0047】

开始设备访问用接收的地址访问的使用通行证存储区域，并且在检查使用通行证的记录状态之后，设立使用通行证状态中的结果。下一步，开始设备连接 UPID、涉及被搜索的使用通行证的解密使能条件、产生的使用通行证状态和使用通行证的记录目标地址，并且将连接的数据传输到原始设备。在连接的数据的传输之前，已从数据自身中计算的散列值、第 m 阶原始会话密钥以及第 n－1 阶开始设备会话密钥，也会进一步连接到上述数据。在这个时间点共享的最新开始会话密钥将为第 n－1 阶。

【0048】

原始设备检查接收的散列值，并且检验接收的数据未被伪造而且以前向开始设备传送的使用通行证在过去的传送（传输）期间是否状态已改变。与所述检验同时，开始设备产生第 n 阶开始会话密钥。在

产生这个密钥之后，开始设备通过使用第 n－1 阶开始会话密钥和第 m 阶原始会话密钥来加密该密钥，并且将加密的数据传输到原始设备。

【0049】

在接收到数据之后，如果原始设备确认，在上述检验期间，使用通行证的状态已被过去传输的执行改变，则原始设备执行下述使用通行证恢复过程。首先，原始设备用第 m 阶原始会话密钥和第 n－1 阶开始会话密钥加密接收的数据。下一步，原始设备向使用通行证的 UPID 连接已在以前的搜索期间检测到的事项记录中记录的解密使能条件，并且通过使用第 n 阶开始会话密钥和对称开始设备密钥来加密连接的数据。在加密之后，原始设备将数据传输到开始设备。

【0050】

然后开始设备通过使用对称开始设备密钥和第 n 阶开始会话密钥来解密接收的数据。在那之后，开始设备确认解密结果中包括的 UPID 是否与将要恢复的使用通行证的 UPID 一致。如果确认了 UPID 之间的一致性，则在存在于开始设备中的使用通行证上通过重写记录解密结果中包括的解密使能条件。

上面是 BT 方式的 BT IP 传送阶段期间的使用通行证恢复过程。这个过程自身被称作 BT IP 恢复阶段。当这个阶段完成时，进行上述传送过程之前存在的使用通行证将存在于原始设备中。

检验被继之以搜索包括接收的 UPID 的原始事项记录。当发现所述记录时，在使用通行证发送模块中现存的使用通行证上重写所述记录中记录的以前传送的解密使能条件。

上面是 BT 方式的 BT PI 传送阶段期间的使用通行证恢复过程。这个过程自身被称作 BT PI 恢复阶段。当这个阶段完成时，在进行上述传输过程之前存在的使用通行证将存在于原始设备中。

【0051】

在下文中对附图进行参考，来说明本发明的实施例。

（系统配置）

首先，使用图 1 和 2，在下面说明包括数据记录/再现装置（记录器/播放器）和可与其连接的存储装置的实施例中的系统的总体配置。

下面说明的实施例是应用于记录/回放系统的例子，通过它，广播数字视频数据、从分发服务器递送的数字数据、或经由连接到外部设备的数字信号线传输的数字数据，记录在可移动的存储装置中，并且使用记录器/播放器的显示装置、扬声器、或其他组元再现存储装置之内存储的数字数据。在下文中，这种数字数据记录器/播放器将被简单地称作记录器/播放器，并且记录器/播放器接收的视频、音乐素材、文本和其他数字数据将被称作内容数据。在本实施例中，用于记录内容数据的可移动存储装置例如是磁盘驱动器、半导体存储装置等，并且这些元件中的任何一种都具有本发明特有的控制功能。下面给出的说明拿磁盘驱动器作为存储装置的例子，但是并未限制本发明。具有下面将说明的本发明的特有功能的任何这样的装置，作为除了磁盘驱动器之外的众所周知的存储装置也能够被应用。

【0052】

需要保护版权的内容数据，在经由广播电波被天线 131 接收之后，或者从分发服务器 150 经由网络接口 100 被接收之后，被获取到记录器/播放器 112 中。递送的内容数据将会借助于需要的的加密方案已在广播电波发送器 130 或分发服务器 150 中被加密。可以根据特殊内容保护规格在它自己之上预先规定加密方案。在上述获取期间，用于解密内容数据的密钥数据（在下文中被称作“内容密钥”）和关于内容数据的使用条件也从内容数据分开地被传输到记录器/播放器 112。用于解密内容数据的这些信息在下文中将被称作“用于内容数据的解密控制信息”。解密控制信息可以从与内容数据相同的传输源传输，或者可以从其他的传输源传输。

【0053】

构造记录器/播放器 112，以便允许例如磁盘驱动器 125、126 的可

移动存储装置的连接。用广播电波传输的或者从分发服务器 150 传输的加密内容数据，以及用于内容数据的解密控制信息，经由记录模块 102 和保护信息传输模块 104，记录在磁盘驱动器 125 和 126 中。同样，加密内容数据和用于内容数据的解密控制信息被从可移动的磁盘驱动器 125 和 126 经由保护信息传输模块 104 传输到回放模块 103。内容数据经由记录器/播放器 112 之内的回放模块 103 被解密并再现。

【0054】

为了防止内容数据的未被授权的使用，解密控制信息中包括的内容密钥必须是这样的：所述密钥不会以未被授权的形式或通过未被授权的手段被取出，或者是这样的：使用条件不会以未被授权的形式或通过未被授权的手段被复制或伪造。因为这些原因，重要的是，用于发送/接收解密控制信息以及记录和读出信息的部件应当安装在记录器/播放器 112 和可移动的磁盘驱动器 125 与 126 中以便具有抗干扰性。这样的部件对应于记录器/播放器 112 中的主机安全管理器 111 或每个磁盘驱动器中的存储安全管理器 225。主机安全管理器 111 之内的保护信息存储 101 的功能，以及每个都位于存储安全管理器 225 里面的使用通行证传送模块 221、限定存储控制器 222 和限定存储器 223 的详细功能，将在稍后说明。根据本发明的实施例涉及传送协议，用于在存在于主机安全管理器 111 和存储安全管理器 225 里面的模块之间交换解密控制信息。顺便提及，或者硬件或者软件可以用于构造记录器/播放器 112 和磁盘驱动器 125、126 里面每个模块的功能以及安全管理器等的功能。

【0055】

与此同时，在记录器/播放器 112 中，用于连接到网络的网络接口 100、网络接口 100 和输入装置之间的接口网桥 105、用于连接到磁盘驱动器的接口 106 和 107、用于控制这些系统部件的处理器或处理单元（PU）、以及其他部分，一起作用以控制系统之内的数据流处理和递送。在这个意义下，在下文中，这些组元将被集体地称作主机模块 110。

【0056】

（模块间相互认证和使用通行证传送方案的综述）

和广播电波一起传输的内容数据，以及其他介质之内记录的内容数据，典型地使用各自规定的方案被加密。这样种类的数据通常也包含各自的解密控制信息。当记录器/播放器 112 经由天线 131 或数字信号线 132 获取这些种类的数据时，记录模块 102 根据规定的方案解密内容数据并检索解密控制信息。检索的解密控制信息被布置到具有本实施例中规定的特定格式的一组数据中。这组数据将在下文中被称作使用通行证。稍后将使用图 4 说明使用通行证的详细结构。

【0057】

记录模块 102 在产生使用通行证之后将所述通行证传输到磁盘驱动器 125 或 126。然而，在传输能够完成之前，必须在记录模块 102 或保护信息传输模块 104 和使用通行证传送模块 221 之间完成相互认证。当认证过程完成时，几组密钥数据被共享。在使用共享密钥加密之后，将要传送的使用通行证被从记录模块 102 传输到使用通行证传送模块 221。

【0058】

本发明涉及认证过程以密钥共享的方法，并且涉及用认证过程期间共享的密钥加密使用通行证并传送加密的使用通行证的处理方法。有两种处理方法。一种是这样的方法，其中，一旦任何两个模块之间的相互认证已完成，就唯一地规定使用通行证的传送方向。另一种方法使得可以双向传送使用通行证。在下文中，使用前者方法的相互认证和使用通行证传送方案将被称作单向传送方式（缩写为 UT 方式），而使用后者方法的相互认证和使用通行证传送方案将被称作双向传送方式（缩写为 BT 方式）。这些方式将集体地被称作限定访问方式。在记录器/播放器的启动期间，主机模块 110 确定两种方式中的哪一种会被用于进行相互认证和当在模块之间传送使用通行证时使用通行证的传送。

【0059】

在磁盘驱动器中，使用通行证传送模块 221 在接收到使用通行证之后将所述通行证传输到限定存储控制器 222。限定存储控制器是控制限定存储器 223 的模块。使用通行证使它的主体最终记录在限定存储

器 223 中。当分发服务器 150 向磁盘驱动器传输使用通行证时，或者当从一个磁盘驱动器向另一个磁盘驱动器传送使用通行证时，依据本发明中规定的任一方案，用于传送使用通行证的模块也许能直接向传送目标磁盘驱动器之内的使用通行证传送模块传输使用通行证。在那种情况下，记录器/播放器 112 里面的网络接口 100 和记录模块 102 仅控制数据从一个模块向另一个模块的传送，并且不直接涉及相互认证或使用通行证的加密。

【0060】

下一步，下面参考图 2 说明磁盘驱动器的构造。

数据经由接口 220 被输入到磁盘驱动器/从磁盘驱动器输出。当除了要被保护的数据之外的数据，诸如使用通行证之类，被从外面输入时，输入的数据经由控制器 230 从磁头 202 记录在磁盘 200 上。加密的内容数据根据数据的流动也记录在磁盘 200 上。当读出时，所述数据与上述说明相反地流动。控制器 230 自身由处理器或处理单元（PU）231 控制。使用通行证传送模块 221、限定存储控制器 222 等也由处理器 231 控制。尽管限定存储器 223 在图 2 中独立于磁盘 200 提供，但是限定存储器可以在磁盘 200 上提供，只要允许仅使用不同于读写加密内容数据的特殊访问方法的访问，并且只要磁盘驱动器被构造以便防止诸如其用于直接读出内部数据的反汇编之类的操作。

【0061】

（系统密钥和数据的结构）

图 3 显示了当使用通行证在记录模块 102 或回放模块 103 和使用通行证传送模块 221 之间传送时用于加密所述通行证的密钥数据的清单。这个清单还包含诸如递送的数据之类的其他数据。通常，当密钥数据 X 是用于对称加密的密钥数据时，使用密钥数据 X 加密将要加密的数据，并且预期数据的解密也使用密钥数据 X。然而，当密钥数据 X 是用于非对称加密的私有密钥或公共密钥时，使用不同于密钥数据 X 的相关公共密钥或私有密钥 Y 加密将要加密的数据。使用密钥数据 X 解密使用私有密钥 Y 加密的数据。在下文中，用于非对称加密的公共

密钥数据将被简单地称作公共密钥，用于非对称加密的私有密钥数据被称作私有密钥，而用于对称加密的密钥数据则被称作对称密钥。如果电子签名伴随着数据，则这意味着其中的一部分包括所述数据的数据集的散列值用适合于公共密钥 X 的私有密钥 Y 加密。

在这个说明书中表示 K_x 的地方，K_x 中的“x”被表示为所有附图中的下标。

【0062】

以下作为涉及内容数据的加密、解密和再现、涉及使用通行证的加密和解密、以及涉及记录模块 102、回放模块 103、磁盘驱动器 125 与 126 和分发服务器 150 的认证的密钥是可用的：

用于加密和解密内容数据的密钥是内容密钥 K_c。用于独立认证的特定的电子签署的公共密钥 KP_dc 被分配给每个分发服务器 150、记录模块 102、回放模块 103 和使用通行证传送模块 221。然而，当整个主机安全管理器 111 要被作为抗干扰的一个功能单元安装时，对于主机安全管理器 111，一个 KP_dc 可以是可分配的。

【0063】

用公共密钥 KP_dc 加密的数据能够用相关的私有密钥 K_dc 解密。一组私有密钥数据被分配给明确数目的分发服务器 150、记录模块 102、回放模块 103 和使用通行证传送模块 221 中的每一个。所述明确数目在这里是指服务器或模块的数目能够是一个或多个。在 KP_dc 和 K_dc 之间共享的单元将被称作类别。用于传送或记录使用通行证的部分的安全级别在安装时必须满足，并且为一个类别规定一个使用通行证传送方案。换言之，属于类别的多个模块全部以这样的形式安装：它们满足为所述类别规定的安全级别，并且这些模块中的每一个都具有用于实现一个共同的使用通行证传送方法的功能。这样的设备和模块在下文中将被集体地称作“设备”。

【0064】

在连接到其他通用信息之后，KP_dc 由需要的的证书机构分配电

子签名，并且执行用于每个设备的证书的功能。用于分配电子签名的证书机构的公共密钥将被称作 KP_CA，而与这个公共密钥相关的私有密钥则被称作 K_CA。在下文中，前者密钥和后者密钥将被分别称作证书机构公共密钥和证书机构私有密钥。证书中包含的通用信息是指证书中的发布源、序列号和其他信息。指示 KP_dc 有效性的证书将被称作设备类别证书，公共密钥 KP_dc 将被称作设备类别公共密钥，而用于解密密钥加密的数据的私有密钥则将被称作设备类别私有密钥。设备类别证书和设备类别私有密钥在发货期间嵌入在每个设备的固有数据中。

独立的公共密钥 KP_d 和用于解密密钥加密的数据的私有密钥 K_d 也嵌入在每个设备的固有数据中。在下文中，前者密钥和后者密钥将被分别称作设备公共密钥和设备私有密钥。嵌入的设备公共密钥和设备私有密钥将从设备到设备而变化。

在用公共密钥加密期间，从用于加密的公共密钥中生成一个对称密钥。这个对称密钥被表示为*KP_d。类似地，在用私有密钥解密期间，从用于解密的私有密钥中生成一个对称密钥。这个对称密钥被表示为*K_d。事实上，*KP_d 和*K_d 是相同的值，并且用*KP_d 加密的数据能够用*K_d 解密。所述两个对称密钥将被分别称作对称设备公共密钥和对称设备私有密钥。在公共密钥加密方法的稍后说明期间将进一步详述生成这些密钥的方法。

【0065】

除了上述之外，在图 1 的系统中使用了对称密钥 K_sn（n>/=0）和对称密钥 K_ch。每次在两个不同的设备之间传送使用通行证，K_sn（n>/=0）都主要在使用通行证传送目标处生成，以便加密使用通行证，并且生成 K_ch 以加密设备之间的相互认证的最终阶段期间在两个设备之间共享的 K_s0。密钥 K_ch 和 K_s0 在设备之间的相互认证期间被共享，并且不用于在其传送期间加密使用通行证。然而，K_sn（n>/=1）总是在每次传送使用通行证时被从 K_sn 更新到 K_sn+1 之后使

用。在下文中，K_ch 将被称作质询密钥，而 K_sn（n>/=0）则将被称作会话密钥。特别地，具有“n”等于 0 的会话密钥将被称作第零阶会话密钥。

【0066】

[P]或[I]的下标被分配给每个密钥。所述下标指示密钥是已被原始设备还是开始设备生成（或嵌入）。原始设备在这里是指任何两个设备中的这样的设备，所述设备在当在两个设备之间进行相互认证时采取的第一个过程步骤中，执行从另一个设备传输的设备类别证书的检验。类似地，开始设备是指执行其固有设备类别证书向另一个设备的传输的设备。

【0067】

使用上述密钥的加密被表示为 E（X，Y），其指示数据 X 使用密钥数据 Y 被加密。同样地，使用密钥解密被表示为 D（X，Y），其指示数据 Y 使用密钥数据 X 被解密。同样，H（X）指示数据 X 的散列值，而 X||Y 则指示数据 X 和数据 Y 被连接在一起。这些表示对 UT 方式和 BT 方式两者都是共同的。

在 UT 方式下，如前所述，使用通行证的传送方向被唯一规定，并且这个方向总是从原始设备向开始设备。因此，在 UT 方式下，记录模块 102 总是作为原始设备操作，而回放模块 103 则总是作为开始设备操作。与此同时，磁盘驱动器当磁盘驱动器记录从记录模块传输的使用通行证时作为开始设备操作，而当磁盘驱动器自身为了例如解密/再现内容数据起见而向回放模块传输使用通行证时则作为原始设备操作。

【0068】

在 BT 方式下，具有主机安全管理器的设备总是作为原始设备操作，而磁盘驱动器则总是作为开始设备操作，并且在这种方式下，使用通行证能够从原始设备向开始设备传送，或者从开始设备向原始设备传送。

【0069】

（使用通行证结构）

下面使用图 4 说明使用通行证的结构。

使用通行证包括：使用通行证格式 400，其指示使用通行证自身能够被输出到哪种模块；标识符 UPID 401，其被唯一地分配给特殊的使用通行证；条件 402 和 404，用于限定将要传送的内容数据的使用；密钥数据 K_c 403，用于译解加密的内容数据；标识符 CID 405，用于识别特殊的内容数据；以及有关内容的版权信息 406。存在两种条件用于限定预期内容数据的使用。一种是控制信息 UR_s 4020，其用于使用通行证的传送源以翻译其细节并控制其输出（记录模块或磁盘驱动器通常能够是使用通行证传送源）。另一种是控制信息 UR_p 4040，其用于回放模块 103 以接收使用通行证和内容数据，然后在模块中控制内容数据解密过程。控制信息 UR_p 4040 包括诸如以下之类的信息：生成计数，其指示有关使用通行证的复制的生成信息；复制计数，其指示模块自身能够如何频繁地复制使用通行证；以及播放计数，其指示模块能够如何频繁地使用其固有使用通行证解密内容数据。

【0070】

（能够在 UT 方式下执行使用通行证传送的使用通行证传送模块的结构）

下面使用图 5 说明能够在 UT 方式下执行使用通行证传送的使用通行证传送模块 221 的结构。

使用通行证传送模块 530 包含：模块 500，其具有用于在关于任何其他设备相互认证之前模块自身作为原始设备进行需要的处理的功能；模块 501，其具有用于模块自身作为原始设备传送使用通行证的功能；模块 502，其具有用于模块自身作为开始设备进行需要的处理的功能；模块 503，其具有用于模块自身作为开始设备接收使用通行证的功能；静态存储区域 504，其中用户不能根据她/他的自行处理更新数据；模块 505，其具有使用通行证恢复功能，以避免传送源设备和传送目标设备两者中使用通行证的丢失，如果用于使用通行证的传送过程的执

行获致异常终止的话；以及使用通行证缓冲器 510，用于在使用通行证被传输到限定存储控制器 222 之前临时存储所述通行证，并且用于临时存储已从限定存储器中读出的使用通行证。

用于认证的模块 500 和 502、用于加密并传输使用通行证的模块 501、用于接收并解密使用通行证的模块 503、用于恢复使用通行证的模块 505 等等，每个都在需要的时访问存储区域 504。存储区域 504 被称作保护信息存储区域。

经由接口 520 和总线 540 进行磁盘驱动器的外面和这些模块中的任何一个之间的数据交换。PU 521 与图 2 的处理器 231 相同。

【0071】

在相互认证过程和使用通行证传送过程的进一步的详细说明中，将经由附图 17 至 20 详述每个模块实际具有的功能。稍后使用图 9 来说明保护信息存储区域 504 中记录的数据种类。

【0072】

（能够在 UT 方式下执行使用通行证传输的记录器/播放器的记录模块的结构）

下面使用图 6 说明能够在 UT 方式下执行使用通行证传输的记录模块 102 的结构。当使用记录器/播放器实现用于在 UT 方式下传送使用通行证的功能时，图 1 中的保护信息传输模块 104 未被显示，因为这个模块并不总是需要的。

在 UT 方式下，记录模块总是作为原始设备操作。因此，记录模块 625 包含：模块 600，其具有用于在关于任何其他设备相互认证之前模块自身作为原始设备进行需要的处理的功能；模块 601，其具有用于模块自身作为原始设备传送使用通行证的功能；模块 605，其具有使用通行证恢复功能，以避免传送源设备和传送目标设备两者中使用通行证的丢失，如果用于使用通行证的传输过程的执行获致异常终止的话；以及模块 606，其具有以下功能：从外面获得内容数据和使用权利信息，

然后在生成内容密钥并用所述密钥加密内容之后，生成包括所述密钥的使用通行证。加密的内容被从模块 606 发送到数据总线 640，并且经由外部存储接口 620 记录在磁盘驱动器中。

【0073】

包括记录模块的主机安全管理器 630 具有静态存储区域 604，其中，用户不能根据她/他的自行处理更新数据。用于认证的模块 600、用于加密并传输使用通行证的模块 601、用于恢复使用通行证的模块 605 等等，每个都在需要的时访问所述存储区域。存储区域 604 被称作保护信息存储区域。

在相互认证过程和使用通行证传送过程的进一步的详细说明中，将经由附图 17 至 20 详述每个模块实际具有的功能。稍后使用图 8 来说明保护信息存储区域 504 中记录的数据种类。

【0074】

（能够在 UT 方式下执行使用通行证接收的记录器/播放器的回放模块的结构）

下面使用图 7 说明能够在 UT 方式下执行使用通行证接收的回放模块 103 的结构。当使用记录器/播放器实现用于在 UT 方式下传送使用通行证的功能时，图 1 中的保护信息传输模块 104 未被显示，因为这个模块并不总是需要的。

【0075】

在 UT 方式下，回放模块总是作为开始设备操作。因此，回放模块 725 包含：模块 702，其具有用于在关于任何其他设备相互认证之前模块自身作为开始设备进行需要的处理的功能；模块 703，其具有用于模块自身作为开始设备接收使用通行证的功能；模块 605，其具有使用通行证恢复功能，以避免传送源设备和传送目标设备两者中使用通行证的丢失，如果用于使用通行证的接收过程的执行获致异常终止的话；以及模块 706，其具有以下功能：从接收的使用通行证中翻译使用通行证中包括的 UR_p 中包含的数据，并且根据 UR_p 解密加密的内容数据。

此时，加密的内容数据经由外部存储接口 720 和数据总线 740 被传输到模块 706。以通过保护数据通信路径的通道的形式，将解密的内容数据从模块 706 直接输出到回放模块的外面。

【0076】

包括回放模块的主机安全管理器 730 具有静态存储区域 704，其中，用户不能根据她/他的自行处理更新数据。用于认证的模块 702、用于接收并解密使用通行证的模块 703、用于恢复使用通行证的模块 705 等等，每个都在需要的时访问所述存储区域。存储区域 704 被称作保护信息存储区域。

在相互认证过程和使用通行证传送过程的进一步的详细说明中，将经由附图 17 至 20 详述每个模块实际具有的功能。稍后使用图 8 来说明保护信息存储区域 504 中记录的数据种类。

【0077】

（在主机安全管理器中，用于 UT 方式的保护信息存储区域的结构）

下面使用图 8 说明记录器/播放器中的用于 UT 方式的保护信息存储区域的结构。存储区域 819 是记录模块 102 访问的区域，而存储区域 839 则是回放模块 103 访问的区域。相同种类的数据保持或记录在存储区域 819 和 839 中。下面说明所述数据。参考数字 801 和 821 指示设备类别清单。设备类别证书 801 包括设备类别公共密钥 800。类似地，设备类别证书 821 包括设备类别公共密钥 820。设备类别清单用于证明证书中包括的设备类别公共密钥的有效性，并且这些证书每个都包括电子签名。电子签名部分用证书机构私有密钥 K_CA 加密。

【0078】

参考数字 803 和 823 指示证书机构公共密钥，804 和 824 指示设备类别私有密钥，805 和 825 指示设备公共密钥，而 806 和 826 则指示设备私有密钥。

上述证书和密钥信息在初始安装期间嵌入，并且它们以后不被更

新。

【0079】

与上面形成对照，被指示为 802、822、810、811、830 和 831 的信息，在相互认证过程和/或使用通行证传送过程期间被更新。被指示为 802 和 822 的信息是撤销设备类别的清单。这个清单被称作 RDCL。如果设备类别公共密钥 KP_dc 的安全性丧失，则在所述清单上登记包括 KP_dc 的证书的特征数。当已从任何其他设备发送的设备类别证书的有效性被检验时，使用电子签名部分确认证书是否被伪造。是否在所述清单上登记了证书的特征数也被确认。同样地，参考数字 810、811、830、831 指示被称作“事项记录”的存储区域。事项记录中的每一个都包含将要传送的使用通行证的 UPID，以及在相互认证中从对方传输的设备类别证书中包括的“有关可接收的使用通行证格式的信息”。只有原始设备记录涉及可接收的使用通行证格式的信息，并且所述信息在下文中将被称作“类型图”。执行相互认证的另一个设备的设备公共密钥（只有开始设备记录公共密钥）、传送期间产生的会话密钥、被称作“会话状态”的使用通行证传送过程的进展、在执行传送之前存在的 UR_s 信息（只有原始设备记录 UR_s 信息）、以及使用通行证的当前记录地址或记录目标地址，在执行使用通行证传送时被记录。在使用通行证传送过程的每个阶段记录这些种类的数据，使得即使使用通行证由于偶发事件等在传送源和传送目标两者中丢失，也可以恢复使用通行证。在相互认证过程和使用通行证传送过程的进一步的详细说明中，将经由附图 17 至 20 详述记录这些种类的数据的时刻。

【0080】

下面说明类型图。如上所述，类型图指示“有关可接收的使用通行证格式的信息”。所述信息包含在设备类别证书中，并且在这个意义下，在认证过程期间，所述信息被发送到在认证中成为对方的设备。在认证中成为对方的设备使用类型图判断另一个设备在该设备是使用通行证传送源时能够接收什么种类的使用通行证。例如，如果使用通行证的使用通行证格式指示“类型 0”，则当在认证中从对方传输的设备类别证书之内的类型图“不能接收类型 0”时，传送使用通行证的设

备不进行使用通行证传送过程。

【0081】

在图 8 中，保护信息存储区域被分成用于记录模块的存储区域和用于回放的存储区域，并且这些区域被构造，以便设备类别证书、证书机构公共密钥、设备类别私有密钥、设备公共密钥、设备私有密钥、事项记录的记录区域、撤销设备类别清单等等记录在特殊区域中。然而，这些存储区域不必需要以那种形式布置。换言之，存储区域可以被布置，以便记录模块和回放模块两者使用一个设备类别证书、一个证书机构公共密钥、一个设备类别私有密钥、一个设备公共密钥和一个设备私有密钥，并且事项记录的记录区域和 RDCL 记录区域可以被布置为可共享的区域。

【0082】

（存在于使用通行证传送模块中的保护信息存储区域的结构）

下面使用图 9 说明磁盘驱动器中的用于 UT 方式的保护信息存储区域的结构。如显示的那样，使用通行证传送模块里面提供的保护信息存储区域 504 中记录的数据，与图 8 中的保持并记录用于记录模块的保护信息 819 或者保持并记录用于回放模块的保护信息 839 相同。换言之，提供了两个区域。一个是区域 902，用于嵌入一个设备类别证书 901、一个证书机构公共密钥 903、一个设备类别私有密钥 904、一个设备公共密钥 905 和一个设备私有密钥 906，并且记录一个 RDCL。另一个是用于记录适当数目的事项记录的区域。使用设备类别证书 901 和密钥 903、904、905、906，而不管磁盘驱动器是成为原始设备还是成为开始设备。同样地也适用于事项记录的记录区域。RDCL 更新能够发生，而不管磁盘驱动器是成为原始设备还是成为开始设备。稍后将使用图 17 说明 RDCL 更新标准。

【0083】

（限定存储器 223 的结构）

下面使用图 10 说明限定存储器 223 的结构。存在于磁盘驱动器中的限定存储器 223 是用于记录并保持从记录模块和其他磁盘驱动器发送的使用通行证的部分。使用通行证记录由限定存储控制器 222 控制。

限定存储器 223 包括例如区域 1000、1010、1020，每个用于记录使用通行证的主体，以及例如区域 1001、1011、1021，每个用于记录指示使用通行证的有效性的标记。在下文中，这些标记将被称作有效性指示器标记。区域 1001 中写入的有效性指示器标记指示区域 1000 中写入的使用通行证的有效性，区域 1011 中写入的有效性指示器标记指示区域 1010 中写入的使用通行证的有效性，而区域 1021 中写入的有效性指示器标记则指示区域 1020 中写入的使用通行证的有效性。用于记录使用通行证的一个区域和用于记录有效性指示器标记的一个区域如上所述是成对的，并且类似于上面在限定存储器 223 里面大量提供。当有效的使用通行证被写入到与标记成对的区域中时，指示“有效”的值通过限定存储控制器 222 记录在每个有效性指示器标记区域中。在写入的使用通行证已被输出到回放模块或任何其他磁盘驱动器之后，在相关的区域中记录指示“无效”的值。在完全初始状态下，记录指示“未记录”的值。限定存储器中记录的使用通行证由限定存储控制器 222 读出。

【0084】

（能够在 BT 方式下执行使用通行证传送的使用通行证传送模块的结构）

下面使用图 11 说明能够在 BT 方式下执行使用通行证传送的使用通行证传送模块的结构。

在 BT 方式下，磁盘驱动器总是作为开始设备操作。因此，使用通行证传送模块 1130 包含：模块 1102，其具有用于在关于任何其他设备相互认证之前模块自身作为开始设备进行需要的处理的功能；模块 1103，其具有用于模块自身作为开始设备传送使用通行证的功能；静态存储区域 1104，其中用户不能根据她/他的自行处理更新数据；模块 1105，其具有使用通行证恢复功能，以避免传送源设备和传送目标设备两者中预期使用通行证的丢失，如果用于使用通行证的传送过程的执行获致异常终止的话；以及使用通行证缓冲器 1110，用于在使用通行证被传输到限定存储控制器 222 之前临时存储所述通行证，并且用

于临时存储已从限定存储器中读出的使用通行证。

静态存储区域 1104 被称作保护信息存储区域，如 UT 方式下那样。然而，这个区域中记录的数据稍微不同于区域 504 中记录的数据。用于认证的模块 1100 在需要的时访问所述存储区域。

【0085】

经由接口 1120 和总线 1140 进行磁盘驱动器的外面和这些模块中的任何一个之间的数据交换。PU 1121 与图 2 的处理器 231 相同。每个模块实际上具有的功能、保护信息存储区域 1104 中记录的数据种类、以及其他要素，稍后使用图 15 和图 21 至 26 来说明。

【0086】

（能够在 BT 方式下执行使用通行证传输的记录器/播放器的记录模块的结构）

下面使用图 12 说明能够在 BT 方式下执行使用通行证传输的记录模块 102 的结构。

在 BT 方式下，整个主机安全管理器 111 总是作为原始设备操作，并且使用通行证关于主机安全管理器 111 双向流动。因此适合于构造记录模块 1225，以便这个模块仅包括输出使用通行证所必须的功能，并且以便保护信息传输模块 104 包括其他功能，诸如关于开始设备进行相互认证之类。因此，记录模块包含：模块 1201，其具有用于模块自身作为原始设备传输使用通行证的功能；模块 1205，其具有使用通行证恢复功能，以避免传送源设备和传送目标设备两者中使用通行证的丢失，如果用于使用通行证的传送过程的执行获致异常终止的话；以及模块 1206，其具有以下功能：从外面获得内容数据和使用权利信息，然后在生成内容密钥并用所述密钥加密内容之后，生成包括所述密钥的使用通行证。加密的内容被从模块 1206 发送到数据总线 1240，并且经由外部存储接口 1220 记录在磁盘驱动器中。

【0087】

包括记录模块的主机安全管理器 1230 具有静态存储区域 1204，

其中，用户不能根据她/他的自行处理更新数据。用于认证的模块 1200、用于加密并传输使用通行证的模块 1201、用于恢复使用通行证的模块 1205 等等，每个都在需要的时访问所述存储区域。存储区域 1204 被称作保护信息存储区域。

在相互认证过程和使用通行证传输过程的进一步的详细说明中，将参考附图 22 至 27 详述每个模块实际具有的功能。稍后使用图 15 来说明保护信息存储区域 1204 中记录的数据种类等。

【0088】

（能够在 BT 方式下执行使用通行证接收的记录器/播放器的回放模块的结构）

下面使用图 13 说明能够在 BT 方式下执行使用通行证接收的回放模块 103 的结构。

在 BT 方式下，如同记录模块一样，回放模块总是作为原始设备操作。如记录模块的说明中阐述的那样，保护信息传输模块 104 承担主机安全管理器的功能，其作为原始设备操作以关于开始设备进行相互认证。因此，回放模块 1325 包含：模块 1303，其具有用于模块自身作为原始设备接收使用通行证的功能；模块 1305 和 1301，两者都具有使用通行证恢复功能，以避免传送源设备和传送目标设备两者中使用通行证的丢失，如果用于使用通行证的接收过程的执行获致异常终止的话；以及模块 1306，其具有以下功能：从接收的使用通行证中翻译使用通行证中包括的 UR_p 中包含的数据，并且根据 UR_p 解密加密的内容数据。此时，加密的内容数据经由外部存储接口 1320 和数据总线 1340 被传输到模块 1306。以通过保护数据通信路径的通道的形式，将解密的内容数据从模块 1306 直接输出到回放模块的外面。

【0089】

包括回放模块的主机安全管理器 1330 具有静态存储区域 1304，其中，用户不能根据她/他的自行处理更新数据。用于认证的模块 1302、用于接收并解密使用通行证的模块 1303、用于恢复使用通行证的模块

1305 和 1301 等等，每个都在需要的时访问所述存储区域。存储区域 1304 被称作保护信息存储区域。

在相互认证过程和使用通行证传送过程的进一步的详细说明中，将经由附图 22 至 27 详述每个模块实际具有的功能。稍后使用图 15 来说明保护信息存储区域 1304 中记录的数据种类。

【0090】

（用于 BT 方式的保护信息传输模块的结构）

下面使用图 14 说明用于 BT 方式的保护信息传输模块的结构。

如记录模块和回放模块的说明中阐述的那样，适合于构造保护信息传输模块，以便这个模块关于开始设备执行相互认证。因此，保护信息传输模块 1410 包含：模块 1400，其作为原始设备操作，以关于开始设备执行相互认证；以及模块 1405，其临时保持存在于回放模块 1416 里面的使用通行证接收模块 1403 所产生的最新会话密钥，并且进行向记录模块之内的使用通行证传输模块 1401 的传输。使用通行证接收模块 1403 中最新会话密钥的产生时刻、在使用通行证传输模块 1401 中使用这种会话密钥的方法、以及其他要素，将在使用图 23 和 24 的处理顺序的说明中详述。

【0091】

（在主机安全管理器中，用于 BT 方式的保护信息存储区域的结构）

下面使用图 15 说明记录器/播放器中的用于 BT 方式的保护信息存储区域的结构。BT 方式是如此设计的方案，以致于不管使用通行证传送方向，整个主机安全管理器 111 和磁盘驱动器总是分别作为原始设备和开始设备操作。使用通行证因此在 BT 方式下能够在两个方向上传送。因为这个原因，通过安装记录模块 102 和回放模块 103 以便所述模块两者共享一个保护信息存储区域，记录器/播放器中的静态存储区域通常能够降低尺寸。

【0092】

呈现这样的情形的图 15 显示了具有保护信息存储区域的内部结构。如对于 UT 方式说明的那样，可以为记录模块 102 和回放模块 103 每个提供独立的存储区域，并且可以将设备类别证书和相互认证所需的密钥存储到每个这样的区域中。在这种情况下，记录模块 102 和回放模块 103 两者都将不得不包括用于相互认证的执行模块。这样的情况因此没有在本实施例中说明。

【0093】

参考数字 1501 指示设备类别证书。设备类别证书 1501 包括设备类别公共密钥 1500。用于证明设备类别公共密钥的有效性的设备类别证书还包括电子签名。电子签名部分用证书机构私有密钥 K_CA 加密。

参考数字 1503 指示证书机构公共密钥。1504 指示设备类别私有密钥，1505 指示设备公共密钥，而 1506 则指示设备私有密钥。

上述证书和密钥信息在初始安装期间嵌入，并且它们以后不被更新。

【0094】

与上面形成对照，区域 1502 和 1510 中记录的两种信息分别是 RDCL 和连接记录，其为在相互认证期间被更新的信息。RDCL 中包含的数据的含意和功能与 UT 方式下的相同。连接记录是 BT 方式的特征记录信息。在记录中记录在认证中作为对方操作的设备的设备公共密钥、设备自身和另一个设备生成的第零阶会话密钥、以及类型图。如显示的那样，连接记录并不具有多个条目。在相互认证已在任何两个设备之间执行之后，如果设备中的一个再连接到不同的设备，则会重写连接记录。

【0095】

在区域 1520 和 1521 中记录事项记录。尽管事项记录是使用通行证传送期间更新的信息，但是记录的数据不同于 UT 方式下记录的数据。在 BT 方式下被记录为事项记录的数据包括：将要传送的使用通行证的 UPID；传送的种类（设备自身是使用通行证的传送源还是传送目

标）；在执行传送之前存在的 UR_s（然而，这种情况下的 UR_s 信息，仅当原始设备是使用通行证的传送源时才应用）；以及使用通行证的当前记录地址（然而，仅当原始设备是传送源时）或者其记录目标地址（然而，仅当原始设备是使用通行证的传送目标时）。当执行使用通行证传送时，记录全部上述数据。在使用通行证传送过程期间记录全部上述数据，使得即使使用通行证由于偶发事件等在传送源和传送目标两者中丢失，也可以恢复使用通行证。在使用通行证传送过程的进一步的详细说明中，将经由附图 23、24、26 和 27 详述记录数据的时刻。

【0096】

（存在于使用通行证传送模块中的保护信息存储区域的结构）

下面使用图 16 说明磁盘驱动器中的用于 BT 方式的保护信息存储区域的结构。如前所述，BT 方式是如此设计的方案，以致于不管使用通行证传送方向，整个主机安全管理器 111 和磁盘驱动器总是分别作为原始设备和开始设备操作。使用通行证因此在 BT 方式下能够在两个方向上传送。

如显示的那样，使用通行证传送模块的保护信息存储区域中记录的数据与主机安全管理器 111 中记录的数据相同，除了事项记录之外。更加具体地，参考数字 1601 指示包括设备类别公共密钥 1600 的设备类别证书。参考数字 1603 指示证书机构公共密钥，1604 指示设备类别私有密钥，1605 指示设备公共密钥，1606 指示设备私有密钥，而 1610 则指示连接记录的记录区域。

【0097】

另外，如显示的那样，限定存储器 223 中的保护信息存储区域不包括事项记录的记录区域。这意味着当传送使用通行证时，磁盘驱动器不记录事项记录。存在下述特征：由于记录未被记录，所以与 UT 方式下的磁盘驱动器的传送处理负荷相比，BT 方式下的使用通行证传送期间的磁盘驱动器的处理负荷相应减少。

上述证书和密钥信息在初始安装期间嵌入，并且它们以后不被更新。另外，在关于将要执行使用通行证的设备进行相互认证期间更新连接记录。这些方面与主机安全管理器 111 之内的保护信息存储器 101 的说明中阐述的那些相同。

【0098】

下一步，参考图 17 至 27 来详细地说明主机模块 110、原始设备和开始设备之间进行的相互认证过程和使用通行证传送过程。这些附图显示了主机设备发布的指令、与指令相关联的沿着数据总线流动的数据、以及每个设备或模块所需以接收或传输指令和数据并执行相互认证或使用通行证传送的过程和功能。

【0099】

（使用通行证传送方式设立）

为了设备传送使用通行证，首先需要设立设备是要使用 UT 方式还是 BT 方式执行使用通行证传送，以主机模块 110 作为居间者 (intervener)，用于连接到设备的可移动存储装置 125、126，并且用于设备中固有的主机安全管理器 111。为了实现上述，从发自主机模块的指令的观点显示了每个设备或模块所需的过程和功能，并且在图 17 中显示了与指令相关联流动的数据流。

在图 17 中，为了方便起见，经由主机模块连接的两个设备被称作设备 1 和设备 2。所述两个设备中的两者，或者是主机安全管理器（更加具体地，根据功能，可以代替地使用记录模块或回放模块），或者是两个可移动存储装置中的任何一个里面存在的使用通行证传送模块。换言之，设备 1 和 2 每个都能够是这些模块中的任何一个。

【0100】

首先，主机模块向设备 2 发布取得限定访问方式指令 17000。然后设备 2 发送响应 17001 以向主机模块 110 通知，设备自身是具有在 UT 方式下执行使用通行证传送的功能，还是具有在 BT 方式下执行使用通行证传送的功能，还是具有所述两种功能中的两者。

下一步，主机模块 110 也向设备 1 发布与上述指令相同的指令 17010。如同设备 2 一样，然后设备 1 发送响应 17011 以向主机模块 110 通知，设备自身是具有在 UT 方式下执行使用通行证传送的功能，还是具有在 BT 方式下执行使用通行证传送的功能，还是具有所述两种功能中的两者。

【0101】

用这种方法，主机模块 110 能够知道设备 2 和 1 中提供的使用通行证方式的种类，并且主机模块 110 选择两个设备的方式并为两个设备设立方式。用于设备 2 的开通信道指令 17020 和用于设备 1 的开通信道指令 17030 用于设立方式。与这些指令相关联，用于识别将要用于执行使用通行证传送的限定访问方式的种类的标识符，以及用于当以同时/并行的方式执行多个传送过程时使多个传送过程可分开的标识符，分别作为数据 17021 和数据 17031 被传输到两个设备。这些标识符在下文中被称作信道标识符。在图 17 中，为设备 1 设立的信道标识符被显示为 ID_[D1]，而为设备 2 设立的信道标识符则被显示为 ID_[D2]。

【0102】

上述以同时/并行方式的传输是指例如下述情形下的传输。在建立认证之后，当使用通行证要被传送时，信道 ID 被识别，并且仅在该信道 ID 下进行传送。具体地在 UT 方式下，当数据被从设备 2（磁盘驱动器）读取同时向其写入时，主机模块发布的指令可以采取如交叉存取那样的形式。在图 28 中显示了这种状态。

在图 28 中，提出使用通行证继之以从主机模块向设备 2 的使用通行证传送，而获取使用通行证则继之以从设备 2 向主机模块的使用通行证传送。用粗线显示的指令（亦即被标记为*1、*2、*3 的指令）具有在它们自身中规定的处理顺序，并且即使在以不规则的顺序接收这些指令之后，设备 2 也中止指令。然而，即使在接收用细线显示的指令（亦即被标记为**1、**2、**3 的指令）之后，设备 2 也并不中止这些指令。这是因为，只有当与那些指令中规定的顺序一致地向设备 2

发送用粗线显示的指令时，才不会发生问题。

在这样的情形下，设备 2 使用信道 ID 在用粗线显示的处理系列和用细线显示的处理系列之间区别。换言之，以同时/并行方式处理呈现如上所述那样的情形。更加具体地，指令不是以这样的方式处理：只有首先从头至尾执行用粗线显示的指令，然后在已传送使用通行证之后，才处理用细线显示的指令。代替地，如上所述，作为一个整体处理属于设备的指令，同时一个指令组插在其他指令组之间。上述不限于其中如上所述存在两个处理系列的情况，并且当在相互插入的条件下执行三个或更多处理系列时上述也适用。

【0103】

将说明返回到图 17。更加具体地，信道标识符被使用如下：

假定例如只有一个可移动存储装置连接到记录器/播放器。在这种情形下，为了在 UT 方式下将使用通行证从记录模块写入到存储装置（例如 125；在下文中，存储装置是指装置 125），与此同时同样在 UT 方式下将记录的使用通行证从存储装置 125 读出到回放模块 103 中，存在下述需要：存储装置 125 被如此构造，以致于它能够分开并管理用于所述两个使用通行证的传送过程。分配不同的信道标识符给这样的两个处理系列，使得可移动存储装置可以判断从主机模块 110 传输的指令与所述两个处理系列中的哪个相关联。

设备 1 和 2，在分别接收数据 17021 和数据 17031 之后，在步骤 17022 和 17032 中执行设立信道标识符和与这个标识符相关联的限定访问方式的过程步骤。

【0104】

在已设立信道标识符和限定访问方式之后，进行设备 1 和 2 之间的相互认证 17040，然后继之以实际使用通行证传送过程步骤 17041 的执行。使用图 18 至 27 来说明这些过程步骤的细节。

在完成需要的的使用通行证传送处理之后，主机模块 110 分别向

设备 2 和 1 发布关闭信道指令 17050 和 17060。信道标识符 17051 和 17061 进一步被传输到与这些指令相关联的各自相关设备。在接收到指令之后，设备每个都复位涉及在指令的接收之后已接收到的信道标识符所识别的处理系列的全部状态信息，并且同样地释放信道标识符。

一旦信道标识符已被释放，除非使用开通指令已重新设置信道标识符和限定访问方式，否则即使当在主机设备发布以执行认证和使用通行证传送的指令中指定信道标识符时，设备也会中止指令处理。

【0105】

（以公共密钥加密的方式共享对称设备公共密钥的方法）

在给出涉及相互认证和使用通行证传送的详细处理顺序的说明之前，下面说明本发明的实施例中使用的公共密钥加密方法。

在本实施例中，椭圆编码(elliptic coding)用作公共密钥加密方法。椭圆编码是这样的方法，在所述方法中，向二维椭圆曲线的方程表达的曲线上的定点[基点 G＝（Gx，Gy）]相加点多达“n”次、亦即重复 G 的相加“n”次的算术运算，在加密期间被使用。与常规十进制加法不同，这里使用的加法是这样的：不同于椭圆曲线上的 G 的点被生成作为通过相加 G 整数次获得的结果。

【0106】

在说明中假定了两个设备，即设备 1 和设备 2。同样假定的是，要被加密的消息 M 记录在设备 1 中，并且与公共密钥 KPu 成对的私有密钥 KPr 记录在设备 2 中。在这种假定下，KPr 是自然数，KPu 是椭圆曲线上的坐标点（KPux，KPuy），并且两者和基点在 KPu＝KPr×G 的关系下相连。换言之，KPu 是通过重复基点的相加 KPr 次获得的点。

【0107】

首先说明设备 1 中的加密过程步骤。

（E1）设备 2 将 KPu 传输到设备 1。

（E2）设备 1 生成随机自然数“r”。

（E3）计算“r×G＝R＝（Rx，Ry）”。

（E4）计算“r×KPu=P=（Px，Py）”。

（E5）使用 Px、Py 计算*KPu=f（Px，Py），生成自然数*KPu，其中函数“f”能够是任何预定值。

（E6）使用*KPu 作为对称密钥，对称地编码要被加密的消息 M，然后由此能够获得 E（*KPu，M）。

（E7）在（E3）中获得的数据连接到在（E6）中获得的数据，并且连接的数据被传输到设备 2。更加具体地，传输的数据是 Rx||Ry||E（*KPu，M）。*KPu 被称作“对称设备公共密钥”。

【0108】

下一步说明设备 2 中的解密过程步骤。

（D1）使用 Rx、Ry、KPr 计算 P，然后由此能够获得“KPr×R=KPr×r×G=r×（KPr×G）=r×KPu=P=（Px，Py）。

（D2）使用 Px、Py 计算*KPr，其中*KPr 恰好是与*KPu 相同的值。前者被表示为*KPr 以指示它已使用 KPr 获得。因此，*KPr=f（Px，Py）。

（D3）计算“r×KPu=P=（Px，Py）”。

（D4）使用*KPr 作为对称密钥，对称地编码接收的数据。因此，D（*KPr，E（*KPu，M）），其在本发明中被称作 D（KPr，E（KPu，M）），其中*KPr 被称作“对称设备私有密钥”。

用于共享对称密钥*KPu、*KPr 的上述算法通常被称作 ECDH 算法。

【0109】

在这个说明书中，包括从 E2 到 E7 的全部过程步骤的加密被称作 E（KPu，M）。如果*KPu 已经被计算并且仅执行过程步骤 E6，则这个过程被称作 E（*KPu，M）。类似地，包括从 D1 到 D4 的全部过程步骤的解密被称作 D（KPr，E（KPu，M））。如果*KPr 已经被计算并且仅执行过程步骤 D4，则这个过程被称作 D（*KPr，E（*KPu，M））。

【0110】

（在图 18 至 27 中出现的代码名称缩写的说明）

图 18 至 27 显示了 UT 方式和 BT 方式下的相互认证处理顺序和使用通行证传送处理顺序。在这些附图中，以下代码表示作为缩写而被使用：

ID：使用通行证标识符

DCC：设备类别证书

PD. C. key：原始设备产生的质询密钥

ID. C. key：开始设备产生的质询密钥

PD. S. key：原始设备产生的会话密钥

ID. S. key：开始设备产生的会话密钥

RDCL：撤销设备类别清单

UP：使用通行证

UPL：使用通行证地点的简称。这个代码表示已经记录在原始设备中或者计划记录在开始设备中的使用通行证的地址。编址方法没有在这里指定，因为它从设备到设备而变化。

MUP：屏蔽的使用通行证。这个代码指示通过将使用通行证状态连接到其内容密钥部分用 0 替换的使用通行证获得的使用通行证状态。

AI：行为指示器。指示接收到了加密使用通行证复制、移动和播放指令中的哪一种。细节在图 19、23 和 24 的说明中阐述。

CKS：校验和。从数据中计算然后连接到数据，所述数据是在以加密的形式传送使用通行证期间通过在传送源处将使用通行证和行为指示器连接在一起而获得的。细节在图 19、23 和 24 的说明中阐述。

TL：事项记录

CL：连接记录

TS_UT：UT 方式下使用的事项状态。细节在图 21 的说明中阐述。

TS_BT：BT 方式下使用的事项状态。细节在图 21 的说明中阐述。

状态：

SS：会话状态。使用通行证传送的进展。细节在图 21 的说明中阐述。

UPS：使用通行证状态。指示作为使用通行证搜索或读出操作的结果而检测到的记录的使用通行证的状态。这个代码采取与图 10 中显

示的任一有效性指示器标记相同的值。或者“有效”、“无效”，或者“未记录”被检测作为UPS。

【0111】

（UT方式下的设备间相互认证处理顺序）

下面使用图18说明用于UT方式下的原始设备和开始设备之间的相互认证的处理顺序。

UT方式下的相互认证处理阶段在下文中被称作“UT连接阶段”。例如当原始设备是存储装置125中的模块500而开始设备是存储装置126中的模块502时，两个可移动存储装置之间的使用通行证的传送发生。例如，当记录模块等已重新生成的使用通行证记录在任一可移动存储装置中时，原始设备是模块600而开始设备则是模块502。例如，当存在于磁盘驱动器中的使用通行证被传输到回放模块，并且对内容数据执行解密、再现/回放等时，原始设备是模块500而开始设备则是模块702。这些关系在图19至21中的UT方式下的每个处理顺序的说明中也是相同的。

【0112】

首先，主机模块向开始设备发布获取设备类别证书指令18000。然后开始设备向主机模块110传输设备自身的数据中嵌入的设备类别证书，如参考数字18001所指示的那样。设备类别证书在下文中被称作DCC（K_CA，KP_dc[I]）。用于证明KP_dc[I]的有效性的证书指示电子签名部分使用K_CA被加密。

主机模块110在接收到DCC（K_CA，KP_dc[I]）之后向原始设备发布验证设备类别证书指令18010，然后向原始设备传输DCC（K_CA，KP_dc[I]）（见18012）。

原始设备在接收到DCC（K_CA，KP_dc[I]）之后，执行参考数字18012中显示的一个过程（过程UT 1.1.1）。

过程 UT 1.1.1：被执行以检验 DCC（K_CA，KP_dc[I]）。

检验通过以下完成：检查证书中包含的数据是否被伪造，并且用于识别证书的 DCC（K_CA，KP_dc[I]）中包括的号码是否存在于原始设备自身中记录的 RDCL_[P]中。数据是否被伪造通过以下判断：计算除了电子签名部分之外的包括 KP_dc[I]的全部数据之内的散列值，然后检查散列值是否与当 DCC（K_CA，KP_dc[I]）中的电子签名部分用 KP_CA 解密时所获得的结果一致。如果两者一致，则这表明证书中包含的数据未被伪造。如果识别证书的号码存在于 RDCL_[P]中，则中止认证。

【0113】

当原始设备在检验 DCC（K_CA，KP_dc[I]）时，主机模块 110 等待处理完成，并且向原始设备发布获取原始设备质询密钥 UT 连接指令 18020。原始设备在接收到所述指令之后，执行参考数字 18021 中显示的以下 3 个过程：

过程 UT 1.2.1：产生质询密钥 K_ch[P]。

过程 UT 1.2.2：使用 DCC（K_CA，KP_dc[I]）之内的 KP_dc[I]加密在过程 UT 1.2.1 期间产生的 K_ch[P]密钥。获得的数据是 E（KP_dc[I]，K_ch[P]）。

过程 UT 1.2.3：将设备的固有数据中嵌入的设备类别证书连接到在过程 UT 1.2.2 期间获得的数据。如此获得的数据是 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]）。

【0114】

在过程 UT 1.2.3 期间产生 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]）之后，原始设备将所述数据传输到主机模块（见参考数字 18022）。然后主机模块接收 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]），并且在向开始设备发布提出原始设备质询密钥 UT 连接指令 18030 之后，向其传送接收的数据（见参考数字 18031）。

【0115】

开始设备在接收到 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]）

之后，执行参考数字 18032 中显示的以下 3 个过程：

过程 UT 1.3.1：被执行以检验 DCC（K_CA，KP_dc[P]）。使用与对过程 UT 1.1.1 说明的方法相同的方法进行检验。然而查阅的 RDCL 是 RDCL_[I]。

过程 UT 1.3.2：分开并仅解密接收数据的 E(KP_dc[I], K_ch[P])。解密使用设备自身的保护信息存储区域中嵌入的 K_dc[I]。

过程 UT 1.3.3：检查过程 UT 1.3.2 的执行结果，K_ch[P]是否以恰当的形式包括。检查被进行如下：首先，在过程 UT 1.3.2 的执行之前，特征数在其加密期间连接到 K_ch[P]被指定，然后，如果作为在过程 UT 1.3.2 中解密接收数据的结果而获得所述特征数，则判断所述数据免于被破坏、析构等。

【0116】

当开始设备在执行过程 UT 1.3.1 至 UT 1.3.3 时，主机模块 110 估计处理的完成时刻，并且在适当的时刻发布获取开始设备会话密钥 UT 连接指令 18040。开始设备在接收到所述指令之后，执行参考数字 18041 中显示的以下两个过程：

过程 UT 1.4.1：产生第零阶会话密钥 K_s[I]0。

过程 UT 1.4.2：将设备的固有数据中嵌入的设备公共密钥连接到设备在过程 UT 1.4.1 期间产生的 K_s[I]0，并且用设备在 UT 1.3.1 中接收的 KP_dc[P]进行加密。已经记录在设备的固有区域中的 RDCL_[I]连接到通过加密获得的数据，并且使用在过程 UT 1.3.3 中获得的 K_ch[P]加密通过连接获得的整个数据。最终获得的数据是 E(K_ch[P]，E（KP_dc[P]，K_s[I]0|| KP_d[I] ）||RDCL_[I]）。

【0117】

在 E（K_ch[P]，E（KP_dc[P]，K_s[I]0|| KP_d[I] ）||RDCL_[I]）已在开始设备中产生之后，设备将产生的数据传输到主机模块（见参考数字 18042）。

然后主机模块接收 E（K_ch[P]，E（KP_dc[P]，K_s[I]0||KP_d[I] ）|| RDCL_[I]），并且在向原始设备发布提出开始设备会话密钥 UT 连接

指令 18050 之后，向其传送接收的数据（见参考数字 18051）。

【0118】

原始设备在接收到 E（K_ch[P]，E（KP_dc[P]，K_s[I]0||KP_d[I] ）|| RDCL_[I]）之后，执行参考数字 18052 中显示的以下 5 个过程：

过程 UT 1. 5. 1：通过使用原始设备自身在过程 UT 1. 2. 1 期间生成的 K_ch[P]解密接收的数据。

过程 UT 1. 5. 2：将 RDCL_[I]从过程 UT 1. 5. 1 的执行结果分开，并且检查 RDCL_[I]是否以恰当的形式包括。检查方法与对过程 UT 1. 3. 3 说明的方法相同。

过程 UT 1. 5. 3：将设备的固有区域中记录的 RDCL_[P]的发布日期信息与传输的 RDCL_[I]的发布日期信息相比较。比较假定 RDCL 的发布日期信息包括在其中。作为比较的结果，如果接收的 RDCL_[I]的发布日期信息比设备的固有区域中记录的 RDCL_[P]的更新，则用 RDCL_[I]重写 RDCL_ [P]。

过程 UT 1. 5. 4：通过使用 K_dc[P]解密剩余的数据 E（KP_dc[P]，K_s[I]0||KP_d[I]）。

过程 UT 1. 5. 5：检查 K_s[I]0||KP_d[I]是否以恰当的形式包括在过程 UT 1. 5. 4 中获得的数据中。检查方法与对过程 UT 1. 3. 3 说明的方法相同。

【0119】

当原始设备在执行过程 UT 1. 5. 1 至 UT 1. 5. 5 时，主机模块 110 估计处理的完成时刻，并且在适当的时刻发布获取原始设备会话密钥 UT 连接指令 18060。原始设备在接收到所述指令之后，执行参考数字 18061 中显示的以下两个过程：

过程 UT 1. 6. 1：产生第零阶会话密钥 K_s[P]0。

过程 UT 1. 6. 2：用在过程 UT 1. 5. 5 中接收的第零阶会话密钥 K_s[I]0 加密在过程 UT 1. 6. 1 中产生的 K_s[P]0。获得的数据是 E（K_s[I]0，K_s[P]0）。在这个过程步骤中，作为在过程 UT 1. 5. 3 中 RDCL_[P]的发布日期信息和 RDCL_[I]的发布日期信息之间比较的结果，如果 RDCL_[P]的发布日期信息比 RDCL_[I]的更新，则 RDCL_[P]

连接到 E(K_s[I]0,K_s[P]0),然后用在过程 UT 1.5.5 中获得的 KP_d[I]加密如此获得的整个数据。最终获得的数据是 E(KP_d[I],E(K_s[I]0,K_s[P]0||KP_d[P])||RDCL_[P])。

【0120】

在 E(KP_d[I],E(K_s[I]0,K_s[P]0||KP_d[P])||RDCL_[P])已在原始设备中产生之后,设备将产生的数据传输到主机模块 110(见参考数字 18062)。

然后主机模块 110 接收 E(KP_d[I],E(K_s[I]0,K_s[P]0||KP_d[P])||RDCL_[P]),并且在向开始设备发布提出原始设备会话密钥 UT 连接指令 18070 之后,向其传送接收的数据(见参考数字 18071)。

【0121】

开始设备在接收到 E(KP_d[I],E(K_s[I]0,K_s[P]0||KP_d[P])||RDCL_[P])之后,执行参考数字 18072 中显示的以下 5 个过程:

过程 UT 1.7.1:通过使用设备的固有保护信息存储区域中嵌入的 K_d[I]解密接收的数据。

过程 UT 1.7.2:如果 RDCL_[P]包括在过程 UT 1.7.1 中解密的数据中,则 RDCL_[P]数据被分开,并且检查所述数据是否以恰当的形式包括。检查方法与对过程 UT 1.3.3 说明的方法相同。

过程 UT 1.7.3:如果在过程 UT 1.7.1 和 1.7.2 的执行之后,RDCL_[P]包括在接收的数据中,并且如果 RDCL_[P]以恰当的形式包括的事实是可确定的,则用接收的 RDCL_[P]重写设备的固有信息存储区域中记录的 RDCL_[I]。

过程 UT 1.7.4:通过使用开始设备自身在过程 UT 1.4.1 期间生成的密钥数据 K_s[I]0 来解密剩余的数据 E(K_s[I]0,K_s[P]0)。

过程 UT 1.7.5:检查 K_s[P]0 是否以恰当的形式包括在过程 UT 1.7.4 中获得的数据中。检查方法与对过程 UT 1.3.3 说明的方法相同。

【0122】

当上述直到 UT 1.7.5 的过程完成时,这就意味着,对称设备公共密钥*KP_d[I](与对称设备私有密钥*K_D[I] 相同)、K_s[I]0 和 K_s[P]0

之间的共享已完成。

【0123】

（UT 方式下的设备间使用通行证传送处理顺序）

在 UT 方式下的原始设备和开始设备之间的相互认证已完成之后，能够从原始设备向开始设备传送使用通行证。下一步使用图 19 来说明使用通行证传送处理顺序。UT 方式下的使用通行证传送处理阶段在下文中被称作“UT 传送阶段”。

【0124】

首先，主机模块 110 向原始设备发布读取使用通行证指令 19000。在这之后，将记录现有使用通行证的地点和将要读出的使用通行证的号码通知给原始设备（见参考数字 19001）。原始设备在接收到上面的指令以及有关现有使用通行证的上述记录地点和有关将要读出的使用通行证的号码的信息之后，执行参考数字 19002 中显示的以下过程：

过程 UT2. 1. 1：在使用通行证传输模块中设立将要传送的使用通行证。例如，如果原始设备是磁盘驱动器，则将要传送的使用通行证的设立相当于将使用通行证从限定存储器 223 经由使用通行证缓冲器 510 发送到模块 501。类似地，如果原始设备是记录模块，则将要传送的使用通行证的设立相当于将使用通行证从限定存储器 223 发送到使用通行证产生器和内容加密器 606。

【0125】

在将要传送的使用通行证已在使用通行证传输模块中设立之后，主机模块 110 向原始设备发布获取屏蔽使用通行证指令 19010。原始设备在接收到这个指令之后，产生屏蔽的使用通行证并将数据传输到主机模块 110（见参考数字 19011）。如前所述，屏蔽的使用通行证是通过将使用通行证状态连接到使用通行证中包括的 0 替换的内容密钥数据而获得的数据。在接收到屏蔽的使用通行证之后，主机模块分析数据中包含的 UR_s，并且判断是否能够传送已被读出到使用通行证传输模块中的使用通行证。如果判断使用通行证是可传送的，则主机模块继续下述使用通行证传送处理。

【0126】

当继续使用通行证传送处理时，主机模块 110 向开始设备发布产生开始设备会话密钥 UT 传送指令 19020。主机模块向开始设备传输将要传送的使用通行证的使用通行证标识符（见参考数字 19021）。开始设备在接收到上述使用通行证标识符之后，执行 19022 中显示的以下 3 个过程：

过程 UT 2. 2. 1：产生会话密钥 K_s[I]n。会话密钥是每次传送使用通行证时产生的对称密钥，并且在那个意义下，K_s[I]n 中的“n”是指密钥已为第 n 个使用通行证传送产生。在那种情况下，“n”>/=1。

过程 UT 2. 2. 2：产生事项记录。在过程 UT 2. 2. 2 中记录将要传送的使用通行证的使用通行证标识符、在过程 UT 2. 2. 1 中产生的会话密钥 K_s[I]n 和会话状态。在单元域(element field)中，设立“RP”（接收准备好）以意指传送目标设备已变得准备好接收使用通行证，并且“U”（未指定）记录在剩余的单元域中。

过程 UT 2. 2. 3：使用在紧接着以前的使用通行证传送的执行期间产生的 K_s[I]n－1，以及通过原始设备在连接阶段产生的第零阶会话密钥 K_s[P]0，加密在过程 UT 2. 2. 1 中产生的会话密钥 K_s[I]n。如果在这个过程的执行之前，没有使用通行证已被传送过，则开始设备使用设备自身在连接阶段的过程 UT 1. 4. 1 中产生的第零阶会话密钥。获得的数据是 E（K_s[P]0，E（K_s[I]n－1， K_s[I]n））。

【0127】

当开始设备在执行过程 UT 2. 2. 1 和 UT 2. 2. 2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取开始设备会话密钥 UT 传送指令 19030。开始设备接收所述指令，然后如参考数字 19031 所指示的那样，向主机模块 110 传输在过程 UT 2. 2. 3 期间产生的数据。

主机模块 110 在接收到 E（K_s[P]0，E（K_s[I]n－1， K_s[I]n））之后，向原始设备发布提出开始设备会话密钥 UT 传送指令 19040，然后将使用通行证标识符连接到接收的数据，并且将连接的数据传输到原始设备（见参考数字 19041）。更加具体地，传输的数据是 UPID‖E（K_s[P]0，E（K_s[I]n－1， K_s[I]n））。

【0128】

原始设备在接收到 UPID‖E(K_s[P]0，E(K_s[I]n－1， K_s[I]n))之后，执行参考数字 19042 中显示的以下 5 个过程：

过程 UT 2.3.1：检查接收的 UPID 和在过程 UT 2.1.1 中的使用通行证传输模块中设立的使用通行证的 UPID 之间的匹配。如果两个 UPID 失配，则使用通行证传送处理在这个阶段中止。

过程 UT 2.3.2：用 K_s[P]0 和 K_s[I]n－1 解密接收的数据，其中，K_s[P]0 是由原始设备自身在过程 UT 1.6.1 中产生的会话密钥，而 K_s[I]n－1 则是与过程 UT 2.2.3 的说明中提到的相同的会话密钥。

过程 UT 2.3.3：检查 K_s[I]n 是否以恰当的形式包括在过程 UT 2.3.2 中获得的数据中。检查方法与对过程 UT 1.3.3 说明的方法相同。

过程 UT 2.3.4：产生事项记录。这个过程中记录的数据包括将要传送的使用通行证的使用通行证标识符、在过程 UT 1.1.1 中获得的开始设备类别证书中包括的类型图、在过程 UT 2.3.3 中产生的会话密钥 K_s[I]n、会话状态、将要传送的使用通行证的 UR_s、以及在过程 UT 2.1.1 中读出的使用通行证的使用通行证地点。在单元域中，设立“SP”（发送准备好）以意指传输设备已变得准备好传输使用通行证。

【0129】

当原始设备在执行过程 UT 2.3.1 至 UT 2.3.4 时，主机模块估计处理的完成时刻，并且在适当的时刻发布加密使用通行证复制、加密使用通行证移动或加密使用通行证播放指令 19050。指令的发布假定全部需要的信息都是预定的。更加具体地，预定的信息是指，例如，在指令接收完成之后，什么 UR_s 被分配给将要传输的使用通行证，并且在复制或回放之后会留在原始设备中的使用通行证的 UR_s 信息要被以什么形式改变。在如此接收所述指令之后，原始设备执行 19051 中显示的以下两个过程：

【0130】

过程 UT 2.4.1：从有关过程 UT 2.1.1 中的使用通行证传输模块中设立的使用通行证的信息中生成将要向开始设备传输的使用通行证。诸如 UPID 和 K_c 之类的信息通常是复制原样的，而只有 UR_s 以

预定形式改变。

过程 UT 2.4.2：指示对于过程 UT 2.4.1 中生成的使用通行证已接收的指令是加密使用通行证复制、加密使用通行证移动还是加密使用通行证播放的行为指示器，以及用于使用通行证||行为指示器的校验和，被计算并连接。在连接之后，使用 K_s[I]n 和*KP_d[I]加密获得的数据。亦即，用对称密钥双重加密数据。获得的数据是 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））。校验和例如将计算如下：首先，根据固定数据长度拆分将要计算的使用通行证||行为指示器。下一步在如此获得的两组数据块相加之后，所有的位值都在极性方面反相，然后进一步加 1。这当然就是指计算包括校验和的整个数据“使用通行证||行为指示器||校验和”的 2 的补码。在检验期间，根据与上述相同的固定数据长度拆分包括校验和的整个数据“使用通行证||行为指示器||校验和”，然后在两组数据块之间进行求和运算。如果相加导致 0，则这表明在检验期间尚未检测到数据变化。

【0131】

当原始设备在执行过程 UT 2.4.1 和 UT 2.4.2 时，主机模块 110 估计处理的完成时刻，并且在适当的时刻发布获取使用通行证指令 19060。在接收到这个指令之后，原始设备执行参考数字 19062 中显示的以下 3 个过程：

过程 UT 2.5.1：更新事项记录中的会话状态。在使用通行证传输完成时，会话状态被设置为“SC”（发送完成）。

过程 UT 2.5.2：在过程 UT 2.4.2 中生成的数据 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））被发送到主机模块。

过程 UT 2.5.3：如预定的那样改变初始使用通行证中的 UR_s。如果原始设备是磁盘驱动器，则用限定存储器中的使用通行证的初始记录地点处的信息重写其 UR_s 已被改变的使用通行证。如果指令 19050 是加密使用通行证移动，则“无效”被设置作为有效性指示器标记的值。

【0132】

主机模块 110 在接收到 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））之后，向开始设备发布提出使用通行证指令 19070，并且向其传输 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））（见 19071）。开始设备在接收到上述指令和数据之后，执行 19072 中显示的以下 3 个过程：

过程 UT 2.5.1：用 K_d[I]和 K_s[I]n 解密接收的数据，其中，K_d[I]是在过程 UT 1.7.1 中获得的会话密钥，而 K_s[I]n 则是设备自身在过程 UT 2.2.1 中生成的会话密钥。

过程 UT 2.5.2：检查使用通行证||行为指示器||校验和是否以恰当的形式包括在过程 UT 2.5.1 中获得的数据中。通过检验校验和并使用对过程 UT 1.3.3 说明的方法来进行检查。使用校验和的检验方法如对过程 UT 2.4.2 说明的那样。

过程 UT 2.5.3：更新事项记录中的会话状态和使用通行证地点。在会话状态中，设立“RC”（接收完成）以意指使用通行证接收已完成。在使用通行证地点域中设立使用通行证的记录目标地址。

【0133】

如果开始设备是磁盘驱动器，则接收的使用通行证在过程 UT 2.5.3 之后记录在限定存储器 223 中。在使用通行证记录期间，有效性指示器标记被设置为“有效”。

在这之后，主机模块 110 可以向开始设备发布检查执行状态指令 19080，以便确认通过开始设备的使用通行证的接收或使用通行证在限定存储器 223 中的记录是否已获致正常结束。在那种情况下，执行状态被作为响应 19081 从开始设备传输到主机模块。

重复上述 UT 传送阶段使得可以连续地执行使用通行证传送而不用重复连接阶段。

【0134】

（UT 方式下的设备间相互再认证处理顺序）

在 UT 传送阶段已在原始设备和开始设备之间重复至少一次、并

且会话密钥 K_s[I]n 已在两个设备之间共享且记录在事项记录中之后，如果记录器/播放器变得异常，并且会话密钥在使用通行证传输模块和接收模块两者中丢失，则相互认证能够在与连接阶段相比的小的处理负荷下重新完成。

下一步使用图 20 来说明这个相互再认证处理顺序。这个 UT 方式下的处理阶段在下文中被称作“UT 再连接阶段”。

【0135】

首先，假定这样的情形给出说明，在所述情形下，在 UT 传送阶段，开始设备在接收提出使用通行证指令 20000 及其后的使用通行证 20001。说明还假定：在使用通行证接收处理被执行到完成之前，由于异常的发生而在原始设备和开始设备之间造成断开，因此，用于加密在被接收的使用通行证 20001 的会话密钥 K_s[I]和对称设备公共密钥 *KP_d[I]在两个设备中丢失（见参考数字 20010）。

在上述情况下，主机模块 110 首先向原始设备发布搜索事项记录再连接指令 20020。在所述指令之后，发送在被传输的使用通行证 20001 的使用通行证标识符（见参考数字 20021）。

原始设备在接收到所述标识符之后，执行参考数字 20022 中显示的以下过程：

过程 UT 3.1.1：为了包含与所述标识符相同的标识符值的事项记录而搜索保护信息存储区域。

【0136】

当原始设备在执行过程 UT 3.1.1 时，主机模块 110 估计处理的完成时刻，并且在适当的时刻发布获取原始设备会话密钥 UT 再连接指令 20030。在接收到这个指令之后，原始设备执行参考数字 20031 中显示的以下两个过程：

过程 UT 3.2.1：产生第零阶会话密钥 K_s[P]0’。

过程 UT 3.2.2：加密在过程 UT 3.2.1 期间产生的 K_s[P]0’。加

密使用在过程UT 3.1.1中检测到的设备的固有事项记录中记录的会话密钥K_s[I]TL和设备公共密钥KP_d[I]TL。密钥K_s[I]TL和KP_d[I]TL指示密钥数据记录在事项记录中。最终获得的数据是E（KP_d[I]TL，E（K_s[I]TL，K_s[P]0’））。

在完成过程UT 3.2.2中的加密之后，原始设备将加密数据传输到主机模块（见20032）。

【0137】

主机模块110在接收到E（KP_d[I]TL，E（K_s[I]TL，K_s[P]0’））之后，向开始设备发布提出原始设备会话密钥UT再连接指令20040，并且在向接收的数据连接与向原始设备传输的使用通行证标识符相同的标识符之后，将连接的数据传输到开始设备（见参考数字20041）。

开始设备在接收到E（KP_d[I]TL，E（K_s[I]TL，K_s[P]0’））之后，执行参考数字20042中显示的以下3个过程：

过程UT 3.3.1：为了包含与所述标识符的值相同的标识符值的事项记录而搜索保护信息存储区域。

过程UT 3.3.2：解密接收的数据。解密使用开始设备的固有保护信息存储区域中嵌入的K_d[I]，以及在过程UT 3.3.1中检测到的事项记录中包括的会话密钥K_s[I]TL。

过程UT 3.3.3：检查作为过程UT 3.3.2执行的结果，K_s[P]0’是否以恰当的形式包括。检查方法与对过程UT 1.3.3说明的方法相同。当过程UT 3.3.2完成时，这表明*KP_d[I]（与*K_d[I]相同）和K_s[P]0’之间的共享已完成。当在上述过程完成之后执行 UT 传送阶段时，K_s[I]TL用作K_s[I]n－1。

【0138】

（UT方式下的使用通行证恢复处理顺序）

在 UT 传送阶段的使用通行证移动期间，在诸如电源故障之类的记录器/播放器异常的情况下，在被传送的使用通行证可能在原始设备和开始设备两者中丢失，或者当将要传送的使用通行证实际上从原始

设备向开始设备传送时，尽管原始设备中的使用通行证的播放计数减少，但是使用通行证可能根本没有在开始设备中再现。以这样的形式提供以使用通行证恢复为特征的系统是重要的：提供初始存在于原始设备中的使用通行证的播放计数。

下一步使用图 21 来说明这样的使用通行证恢复处理。这个 UT 方式下的处理阶段在下文中被称作“UT 恢复阶段”。

【0139】

首先，假定这样的情形给出说明，在所述情形下，在 UT 传送阶段，开始设备在接收提出使用通行证指令 21000 及其后的使用通行证 21001。说明还假定：在使用通行证接收处理被执行到完成之前，由于异常的发生而在原始设备和开始设备之间造成断开，因此，用于加密在被接收的使用通行证 21001 的会话密钥 K_s[I]在两个设备中丢失（见参考数字 21010）。在这种情况下，首先执行在上文中说明的 UT 再连接阶段，并且重新共享*KP_d[I]（与*K_d[I]相同）、K_s[P]0’。

【0140】

在 UT 再连接阶段之后，主机模块 110 首先向开始设备发布搜索使用通行证 UT 恢复指令 21020。在所述指令之后，主机模块 110 发送在被传输的使用通行证 21001 的使用通行证标识符（见 21021）。

开始设备在接收到所述标识符之后，执行参考数字 21022 中显示的以下 4 个过程：

过程 UT 4.1.1：为了包含与所述标识符相同的标识符值的事项记录而搜索保护信息存储区域。

过程 UT 4.1.2：通过在过程 UT 4.1.1 中检测到的事项记录中记录的使用通行证地点指定，搜索限定存储器中的使用通行证存储区域。

过程 UT 4.1.3：检查与在过程 UT 4.1.2 中检测到的使用通行证相关联的有效性指示器标记的值，并且在使用通行证状态中设立“有

效”、“无效”或“未记录”。

过程 UT 4.1.4：产生用于 UT 方式的事项状态。事项状态是在将要传送的使用通行证的“UPID||事项记录”中记录的“会话状态||过程 UT 4.1.3”中设立的“使用通行证状态||散列”值。这里的散列值是从 K_s[P]0'||K_s[I]TL|| UPID||会话状态||使用通行证状态中计算的。已在这个过程期间生成的事项状态在下文中被称作“UT 事项状态”。

【0141】

当开始设备在执行过程 UT 4.1.1 至 UT 4.1.4 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取事项状态 UT 恢复指令 21030。开始设备接收所述指令，然后如参考数字 21031 所指示的那样，向主机模块 110 传输在过程 UT 4.1.4 期间产生的 UT 事项状态。

主机模块 110 在接收到事项状态之后，向原始设备发布检验事项状态 UT 恢复指令 21040，然后传输接收的数据（见 21041）。更加具体地，传输的数据是 UT 事项状态。

【0142】

原始设备在接收到 UT 事项状态之后，执行参考数字 21042 中显示的以下 3 个过程：

过程 UT 4.2.1：检验 UT 事项状态并确认 UT 事项状态中包括的使用通行证标识符、会话状态和使用通行证状态。通过从原始设备的固有信息区域中保持的 K_s[P]0'和 K_s[I]TL 中计算数据中包含的散列值，完成 UT 事项状态的检验。如果计算结果匹配散列值，则判断数据未被伪造。使用通行证标识符用于确认使用通行证是否是要被恢复的，而会话状态和使用通行证状态则用于判断使用通行证是否是可恢复的。如果会话状态是“RP”，或者如果会话状态是“RP”但是使用通行证状态是“无效”或“未记录”，则进行通过原始设备的恢复过程（下面的过程 UT 4.2.2）。

过程 UT 4.2.2：为了包含与所述标识符相同的标识符值的事项记录而搜索保护信息存储区域。

过程 UT 4.2.3：执行使用通行证恢复过程。通过以下完成使用通行证的恢复：将预期使用通行证的有效性指示器标记变为“有效”（如果“无效”的话），并且用在过程 UT 4.2.2 中检测到的事项记录中记录的 UR_s 重写使用通行证的 UR_s。

【0143】

在那之后，主机模块向原始设备发布检查执行状态指令 21050，以确认使用通行证恢复是否从而已获致正常结束。从原始设备向主机模块传输执行状态（见参考数字 21051）。

当过程 UT 4.2.2 完成时，在被传输之前存在的使用通行证将存在于原始设备中。

【0144】

（BT 方式下的设备间相互认证处理顺序）

下面使用图 22 说明用于 BT 方式下的原始设备和开始设备之间的相互认证的处理顺序。BT 方式下的相互认证处理阶段在下文中被称作“BT 连接阶段”。

如每个附图 11 至 13 所述，在 BT 方式下，记录器/播放器里面的整个主机安全管理器 111 作为原始设备操作。在管理器的所有内部模块之中，只有保护信息传输模块 1410 里面的模块 1400 承担相互认证，并且分别只有记录模块或回放模块里面的模块 1201 或 1303 承担使用通行证传输和/或接收过程。同样，磁盘驱动器里面的使用通行证传送模块 1130 作为开始设备操作。这些关系在图 22 至 27 中的 BT 方式下的每个处理顺序的稍后说明中也是相同的。

【0145】

首先，主机模块 220 向开始设备发布获取设备类别证书指令 22000。然后如参考数字 22001 所指示的那样，开始设备将设备的固有数据中嵌入的设备类别证书 DCC（K_CA，KP_dc[I]）传输到主机模块 110。

主机模块 110 在接收到 DCC（K_CA，KP_dc[I]）之后，向原始设备发布检验设备类别证书指令 22010，然后向其传输 DCC（K_CA，KP_dc[I]）（见 22011）。

【0146】

原始设备在接收到 DCC（K_CA，KP_dc[I]）之后，执行 22012 中显示的以下 4 个过程：

过程 BT 1. 1. 1：被执行以检验 DCC（K_CA，KP_dc[I]）。检验是指检查证书中包含的数据是否被伪造，并且用于识别证书的 DCC（K_CA，KP_dc[I]）中包括的号码是否存在于原始设备自身中记录的 RDCL_[P]中。检验方法与对 UT 过程 1. 1. 1 说明的方法相同。

过程 BT 1. 1. 2：产生质询密钥 K_ch[P]。

过程 BT 1. 1. 3：用 DCC（K_CA，KP_dc[I]）中包括的 KP_dc[I] 加密在过程 BT 1. 1. 2 期间产生的 K_ch[P]。加密使用公共密钥编码方案。获得的数据是 E（KP_dc[I]，K_ch[P]）。

过程 BT 1. 1. 4：将设备的固有数据中嵌入的设备类别证书连接到在过程 BT 1. 1. 3 期间获得的数据。获得的数据是 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]）。

【0147】

当原始设备在执行过程 BT 1. 1. 1 至 1. 1. 4 时，主机模块 110 等待处理完成，并且发布获取原始设备质询密钥 BT 连接指令 22030。原始设备在接收到所述指令之后，将在过程 BT 1. 1. 4 期间产生的数据传输到主机模块（见参考数字 22031）。

然后主机模块 110 接收 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]），并且在向开始设备发布提出原始设备质询密钥 BT 连接指令 22040 之后，向其传送接收的数据（见参考数字 22041）。

【0148】

开始设备在接收到 E（KP_dc[I]，K_ch[P]）‖DCC（K_CA，KP_dc[P]）之后，执行参考数字 22042 中显示的以下 3 个过程：

过程 BT 1. 2. 1：被执行以检验 DCC（K_CA，KP_dc[P]）。检验

方法与对过程 UT 1. 1. 1 说明的方法相同。然而查阅的 RDCL 是 RDCL_[I]。

过程 BT 1. 2. 2：分开并仅解密接收数据的 E（KP_dc[I]，K_ch[P]）。解密使用设备自身的保护信息存储区域中嵌入的 K_dc[I]。

过程 BT 1. 2. 3：检查过程 BT 1. 2. 2 的执行结果，K_ch[P]是否以恰当的形式包括。检查方法与对过程 UT 1. 3. 3 说明的方法相同。

【0149】

在过程 BT 1. 2. 1 至 1. 2. 3 的执行期间，主机模块 110 估计处理的完成时刻，并且在适当的时刻发布获取开始设备质询密钥 BT 连接指令 22050。开始设备在接收到所述指令之后，执行参考数字 22051 中显示的以下两个过程：

过程 BT 1. 3. 1：产生质询密钥 K_ch[I]。

过程 BT 1. 3. 2：将设备的固有信息存储区域中嵌入的设备公共密钥 KP_d[I]连接到在过程 BT 1. 3. 1 期间产生的数据，并且用在过程 BT 1. 2. 1 中接收的 KP_dc[P]进行加密。记录在设备的固有信息区域中的 RDCL_[I]连接到通过加密已获得的数据，并且使用在过程 BT 1. 2. 3 中获得的 K_ch[P]加密获得的整个数据。最终获得的数据是 E（K_ch[P]，E（KP_dc[P]，K_ch[I]|| KP_d[I]）||RDCL_[I]）。

【0150】

在 E（K_ch[P]，E（KP_dc[P]，K_ch[I]|| KP_d[I]）||RDCL_[I]）已在开始设备中产生之后，设备将产生的数据传输到主机模块（见参考数字 22052）。

然后主机模块 110 接收 E（K_ch[P]，E（KP_dc[P]，K_ch[I]|| KP_d[I]）||RDCL_[I]），并且在向原始设备发布提出开始设备质询密钥 BT 连接指令 22060 之后，向其传送接收的数据（见参考数字 22061）。

【0151】

原始设备在接收到 E（K_ch[P]，E（KP_dc[P]，K_ch[I]|| KP_d[I]）||RDCL_[I]）之后，执行参考数字 22062 中显示的以下 7 个过程：

过程 BT 1. 4. 1：通过使用设备自身在过程 BT 1. 1. 2 期间生成的

密钥数据 K_ch[P]解密接收的数据。

过程 BT 1.4.2：将 RDCL_[I]从过程 BT 1.4.1 的执行结果分开，并且检查 RDCL_[I]是否以恰当的形式包括。检查方法与对过程 UT 1.3.3 说明的方法相同。

过程 BT 1.4.3：将设备的固有区域中记录的 RDCL_[P]的发布日期信息与传输的 RDCL_[I]的发布日期信息相比较。比较假定 RDCL 的发布日期信息包括在其中。作为比较的结果，如果接收的 RDCL_[I]的发布日期信息比设备的固有区域中记录的 RDCL_[P]的更新，则用 RDCL_[I]重写 RDCL_ [P]。

过程 BT 1.4.4：通过使用 K_dc[P]解密剩余的数据 E（KP_dc[P]，K_ch[I]||KP_d[I]）。

过程 BT 1.4.5：检查 K_ch[I]||KP_d[I]是否以恰当的形式包括在过程 BT 1.4.4 中获得的数据中。检查方法与对过程 UT 1.2.3 说明的方法相同。

过程 BT 1.4.6：产生第零阶会话密钥 K_s[P]0。

过程 BT 1.4.7：将设备的固有信息存储区域中嵌入的设备公共密钥 KP_d[P]连接到在过程 BT 1.4.6 期间产生的 K_s[P]0，并且用在过程 BT 1.4.5 中接收的 KP_d[I]进行加密。如此获得的数据是 E（KP_d[I]，K_s[P]0|| KP_d[P]）。此时，作为过程 BT 1.4.3 中 RDCL_[P]和 RDCL_[I]发布日期信息的比较结果，如果 RDCL_[P]的发布日期更新，则 RDCL_[P]连接到 E（KP_d[I]，K_s[P]0|| KP_d[P]），然后使用在过程 BT 1.4.5 中获得的 K_ch[I]加密如此获得的整个数据。最终获得的数据是 E（K_ch[I]，E（KP_d[I]，K_s[P]0|| KP_d[P]）|| RDCL_[P]）。

【0152】

当原始设备在执行过程 BT 1.4.1 至 1.4.7 时，主机模块 110 估计处理的完成时刻，并且在适当的时刻发布获取原始设备会话密钥 BT 连接指令 22070。原始设备在接收到所述指令之后，将在过程 BT 1.4.7 期间产生的数据 E(K_ch[I]，E(KP_d[I]，K_s[P]0|| KP_d[P])|| RDCL_[P]）传输到主机模块（见参考数字 22071）。

然后主机模块 110 接收 E(K_ch[I], E(KP_d[I], K_s[P]0|| KP_d[P]) || RDCL_[P])，并且在向开始设备发布提出原始设备会话密钥 BT 连接指令 22080 之后，向设备传送接收的数据（见参考数字 22081）。

【0153】

开始设备在接收到 E（K_ch[I]，E（KP_d[I]，K_s[P]0|| KP_d[P]）|| RDCL_[P]）之后，执行参考数字 22082 中显示的以下 5 个过程：

过程 BT 1. 5. 1：通过使用设备自身在过程 BT 1. 3. 1 期间生成的密钥数据 K_ch[I]解密接收的数据。

过程 BT 1. 5. 2：如果 RDCL_[P]包括在过程 BT 1. 5. 1 的执行结果中，则 RDCL_[P]数据被分开，并且检查所述数据是否以恰当的形式包括。检查方法与对过程 UT 1. 3. 3 说明的方法相同。

过程 BT 1. 5. 3：如果在过程 BT 1. 5. 1 和 1. 5. 2 的执行之后，RDCL_[P]包括在接收的数据中，并且如果 RDCL_[P]以恰当的形式包括的事实是可确定的，则用接收的 RDCL_[P]重写设备的固有信息存储区域中记录的 RDCL_[I]。

过程 BT 1. 5. 4：通过使用设备的固有保护信息存储区域中嵌入的 K_s[I]0 来解密剩余的数据 E（KP_d[I]，K_s[P]0|| KP_d[P]）。

过程 BT 1. 5. 5：检查 K_s[P]0|| KP_d[P]是否以恰当的形式包括在过程 BT 1. 5. 4 中获得的数据中。检查方法与对过程 UT 1. 3. 3 说明的方法相同。

【0154】

当开始设备在执行过程 BT 1. 5. 1 至 1. 5. 5 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取开始设备会话密钥 BT 连接指令 22090。开始设备在接收到所述指令之后，执行参考数字 22091 中显示的以下 3 个过程：

过程 BT 1. 6. 1：产生第零阶会话密钥 K_s[I]0。

过程 BT 1. 6. 2：在连接记录上记录在过程 BT 1. 5. 5 期间接收的 K_s[P]0 和 KP_d[P]、在过程 BT 1. 6. 1 期间产生的 K_s[I]0、以及在过程 BT 1. 2. 1 期间接收的 DCC（K_CA，KP_dc[P]）中包括的原始设备的类型图 TM_[P]。

过程 BT 1.6.3：加密在过程 BT 1.6.1 期间产生的 K_s[I]0。加密使用在过程 BT 1.5.5 期间接收的 K_s[P]0 和 KP_d[P]。将要产生的数据是 E（KP_d[P]，E（K_s[P]0，K_s[I]0））。

【0155】

在 E（KP_d[P]，E（K_s[P]0，K_s[I]0））已在开始设备中产生之后，设备将产生的数据传输到主机模块（见参考数字 22092）。

然后主机模块 110 接收 E（KP_d[P]，E（K_s[P]0，K_s[I]0）），并且在向原始设备发布提出开始设备会话密钥 BT 连接指令 22100 之后，向其传送接收的数据（见参考数字 22101）。

【0156】

原始设备在接收到 E（KP_d[P]，E（K_s[P]0，K_s[I]0））之后，执行参考数字 22102 中显示的以下 3 个过程：

过程 BT 1.7.1：通过使用 K_d[P]和 K_s[P]0 来解密接收的数据，其中，K_d[P]是设备的固有保护信息区域中嵌入的密钥数据，而 K_s[P]0 则是设备自身在过程 BT 1.4.6 期间生成的密钥数据。

过程 BT 1.7.2：检查 K_s[I]0 是否以恰当的形式包括在过程 BT 1.7.1 中获得的数据中。检查方法与对过程 UT 1.3.3 说明的方法相同。

过程 BT 1.7.3：在连接记录上记录在过程 BT 1.4.5 期间接收的 KP_d[I]、在过程 BT 1.7.2 期间接收的 K_s[I]0、以及在过程 BT 1.1.1 期间接收的 DCC（K_CA，KP_dc[I]）中包括的开始设备的类型图 TM_[I]。

当直到 BT 1.7.3 的每个过程完成时，这就意味着，对称设备公共密钥*KP_d[P]（与对称设备私有密钥*K_d[P]相同）、K_s[P]0 和 K_s[I]0 之间的共享已完成。

【0157】

（用于 BT 方式下的从原始设备向开始设备的使用通行证传送的处理顺序）

在 BT 方式下的原始设备和开始设备之间的相互认证已完成之后，

使用通行证能够从原始设备向开始设备传送，或反之。

首先使用图 23 来说明从原始设备向开始设备的使用通行证传送。当记录模块 102 作为原始设备操作以向磁盘驱动器传送使用通行证时，一个这样的例子适用。BT 方式下的从原始设备向开始设备的使用通行证传送的处理阶段在下文中被称作“BT PI 传送阶段”。

【0158】

首先，主机模块 110 向原始设备发布读取使用通行证指令 23000。在这之后，将记录现有使用通行证的地点和将要读出的使用通行证的号码通知给原始设备（见参考数字 23001）。原始设备在接收到上面的指令以及有关现有使用通行证的上述记录地点和有关将要读出的使用通行证的号码的信息之后，执行参考数字 23002 中显示的以下过程：

过程 BT 2. 1. 1：在使用通行证传输模块中设立将要传送的使用通行证。如果原始设备是记录模块，则将要传送的使用通行证的设立相当于将使用通行证从使用通行证产生器和内容加密器 606 发送到模块 601。

【0159】

在使原始设备执行过程 BT 2. 1. 1 时，主机模块 110 向开始设备发布产生开始设备会话密钥 UT 传送指令 19020。开始设备在接收到这个指令之后，执行参考数字 23012 中显示的以下两个过程：

过程 BT 2. 2. 1：产生会话密钥 K_s[I]n，其中“n”是指，这个过程是 BT 连接阶段完成之后的第 n 个 BT PI 传送阶段。

过程 BT 2. 2. 2：加密在过程 BT 2. 2. 1 期间产生的 K_s[I]n。加密使用紧接着以前的使用通行证传送的执行期间产生的会话密钥 K_s[I]n－1，以及由原始设备产生的最新会话密钥 K_s[P]m。密钥 K_s[P]m 在每次使用通行证从开始设备向原始设备传送时生成，并且意味着传送过程在 BT 连接阶段完成之后已重复了“m”次。稍后将使用图 24 详细地说明从开始设备向原始设备的使用通行证传送的处理顺序。如果没有使用通行证已从开始设备传送到原始设备，则在 BT 连接阶段共享

的第零阶会话密钥 K_s[P]0 将用作 K_s[P]m。获得的数据将会是 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））。

【0160】

当开始设备在执行过程 BT 2.2.1 和 2.2.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取开始设备会话密钥 BT 传送指令 23020。开始设备在接收到所述指令之后，将过程 BT 2.2.2 期间生成的数据 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））传输到主机模块（见参考数字 23021）。

主机模块 110 在接收到 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））之后，向原始设备发布提出开始设备会话密钥 BT 传送指令 22030，然后向其发送接收的数据（见参考数字 23031）。

【0161】

原始设备在接收到 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））之后，执行参考数字 23032 中显示的以下 3 个过程：

过程 BT 2.3.1：通过使用 K_s[P]m 和 K_s[I]n－1 解密接收的数据。两组密钥数据均如对过程 BT 2.2.2 说明的那样。

过程 BT 2.3.2：检查 K_s[I]n 是否以恰当的形式包括在过程 BT 2.3.1 中获得的数据中。检查方法与对过程 UT 1.3.3 说明的方法相同。

过程 BT 2.3.3：产生事项记录。在 BT 方式下的使用通行证传送过程期间，只有原始设备在事项记录中记录数据。BT 方式下的事项记录的单元是：将要传送的使用通行证的使用通行证标识符；原始设备在使用通行证传送过程中的角色（亦即，是作为使用通行证传送“源”还是“目标”操作）；只有当原始设备是使用通行证传送目标时，在它到达计划接收它的原始设备之前存在的使用通行证的 UR_s，或者只有当原始设备是使用通行证传送源时，在从计划传送使用通行证的原始设备传输之前存在的使用通行证自身；以及只有当原始设备是使用通行证传送目标时，传送源处的使用通行证地点（读出源地址），或者只有当原始设备是使用通行证传送源时，传送目标处的使用通行证地点（记录目标地址）。

在上述之中，只有以下单元记录在事项记录中：将要传送的使用通行证的使用通行证标识符；原始设备在使用通行证传送过程中的角色，亦即“源”（在图 23 中，以缩写的形式显示为“S”）；在传输之前存在的使用通行证自身；以及使用通行证的使用通行证地点（记录目标地址）。

【0162】

当原始设备在执行过程 BT 2. 3. 1 至 BT 2. 3. 3 时，主机模块估计处理的完成时刻，并且在适当的时刻发布加密使用通行证复制、加密使用通行证移动或加密使用通行证播放指令 23040。在所述指令之后，向原始设备传输对开始设备的使用通行证的记录目标地址信息（见参考数字 23041）。在 BT 方式下，如 UT 方式下那样，指令的发布假定所有的需要的信息都是预定的。更加具体地，预定的信息是指，例如，在指令接收完成之后，什么 UR_s 被分配给将要传输的使用通行证，并且在复制或回放之后会留在原始设备中的使用通行证的 UR_s 信息要被以什么形式改变。在如此接收所述指令之后，原始设备执行参考数字 23042 中显示的以下 3 个过程：

过程 BT 2. 4. 1：从有关过程 BT 2. 1. 1 中的使用通行证传输模块中设立的使用通行证的信息中生成将要向开始设备传输的使用通行证。诸如 UPID 和 K_c 之类的信息通常是复制原样的，而只有 UR_s 以预定形式改变。

过程 BT 2. 4. 2：过程 BT 23041 期间接收的开始设备中的使用通行证记录目标地址记录在事项记录中的使用通行证地点处。

过程 BT 2. 4. 3：指示对于过程 BT 2. 4. 1 中生成的使用通行证已接收的指令是加密使用通行证复制、加密使用通行证移动还是加密使用通行证播放的行为指示器，以及用于使用通行证||行为指示器的校验和，被计算并连接在一起。在连接之后，使用 K_s[I]n 和*KP_d[I]加密获得的数据。亦即，用对称密钥双重加密数据。获得的数据是 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））。校验和的计算如对过程 UT 2. 4. 2 说明的那样。

【0163】

当原始设备在执行过程 BT 2.4.1 至 BT 2.4.3 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取使用通行证指令 23050。在接收到这个指令之后，原始设备将 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））传输到主机模块（见参考数字 23052）。主机模块 110 在接收到 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））之后，向开始设备发布提出使用通行证指令 23060，然后向其传送 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））（见参考数字 23061）。

【0164】

开始设备在接收到 E（*KP_d[I]，E（K_s[I]n，使用通行证||行为指示器||校验和））之后，执行参考数字 23062 中显示的以下 3 个过程：

过程 BT 2.5.1：用*K_d[I]和 K_s[I]n 解密接收的数据，其中，*K_d[I]是在过程 BT 1.5.4 中获得的对称密钥，而 K_s[I]n 则是设备自身在过程 BT 2.2.1 中生成的会话密钥。

过程 BT 2.5.2：检查使用通行证||行为指示器||校验和是否以恰当的形式包括在过程 BT 2.5.1 中获得的数据中。通过检验校验和并使用对过程 UT 1.3.3 说明的方法来进行检查。使用校验和的检验方法如对过程 UT 2.4.2 说明的那样。

过程 BT 2.5.3：在限定存储器中记录接收的使用通行证。在使用通行证记录期间，有效性指示器标记被设置为“有效”。

在这之后，主机模块 110 可以向开始设备发布检查执行状态指令 23070，以便确认通过开始设备的使用通行证的接收或使用通行证在限定存储器 223 中的记录是否已获致正常结束。在那种情况下，执行状态被作为响应 23071 从开始设备传输到主机模块。

重复上述 BT 传送阶段使得可以连续地执行使用通行证传送而不

用重复连接阶段。

【0165】

（用于 BT 方式下的从开始设备向原始设备的使用通行证传送的处理顺序）

下一步，使用图 24 来说明从开始设备向原始设备的使用通行证传送。当磁盘驱动器作为原始设备操作以向回放模块 104 传送使用通行证时，一个这样的例子适用。BT 方式下的从开始设备向原始设备的使用通行证传送的处理阶段在下文中被称作“BT IP 传送阶段”。

【0166】

首先，主机模块 110 向开始设备发布读取使用通行证指令 24000。在这之后，将记录现有使用通行证的地点和将要读出的使用通行证的号码通知给开始设备（见参考数字 24001）。开始设备在接收到上面的指令以及有关现有使用通行证的上述记录地点和有关将要读出的使用通行证的号码的信息之后，执行参考数字 24002 中显示的以下过程：

过程 BT 3. 1. 1：从限定存储器中的特定地址中读出将要传送的使用通行证，并且将使用通行证传输到使用通行证缓冲器 1110。

【0167】

当开始设备在执行过程 BT 3. 1. 1 时，主机模块估计处理的完成时刻，并且在适当的时刻向开始设备发布获取具有屏蔽散列的屏蔽使用通行证指令 24010。开始设备在接收到这个指令之后，执行参考数字 24011 中显示的以下两个过程：

过程 BT 3. 2. 1：根据读取使用通行证指令 24000，从读出自限定存储器的使用通行证中的一个中，产生屏蔽的使用通行证，并且从通过连接当获取具有屏蔽散列的屏蔽使用通行证指令 24010 被接收时存在的最新会话密钥 K_s[P]m－1 和 K_s[I]n 而获得的数据中，计算该读取使用通行证的散列值。如果根据读取使用通行证指令 24000 一次读出多个使用通行证，则计算每个使用通行证的散列值。

过程 BT 3. 2. 2：在过程 BT 3. 2. 1 期间生成的散列值连接到各个屏蔽使用通行证。获得的数据是 MUP||H（K_s[P]m－1||K_s[I]n||MUP）。

【0168】

在完成过程 BT 3. 2. 2 之后，开始设备将产生的数据 MUP||H（K_s[P]m－1||K_s[I]n||MUP）发送到主机模块（见参考数字 24012）。

主机模块 110 在接收到 MUP||H（K_s[P]m－1||K_s[I]n||MUP）之后，向原始设备发布提出具有屏蔽散列的屏蔽使用通行证指令，然后向其传输数据。

【0169】

原始设备在接收到数据之后，执行参考数字 24022 中显示的以下过程：

过程 BT 3. 3. 1：检验接收的数据是否被伪造，并且使用接收的 MUP 以及设备自身保持的会话密钥 K_s[P]m－1 和 K_s[I]n，计算散列值 H（K_s[P]m－1||K_s[I]n||MUP）。如果计算结果匹配接收的散列值，则判断接收的数据未被伪造。

当原始设备在执行过程 BT 3. 3. 1 时，主机模块估计处理的完成时刻，并且在适当的时刻向原始设备发布产生原始设备会话密钥 BT 传送指令 24030 之后，传输将要传送的使用通行证的使用通行证标识符（见参考数字 24031）。

【0170】

原始设备在接收到上述指令和数据之后，执行参考数字 24032 中显示的以下 4 个过程：

过程 BT 3. 4. 1：检查在 24031 中接收的使用通行证标识符和在 24021 中接收的屏蔽使用通行证的使用通行证标识符之间的匹配。

过程 BT 3. 4. 2：产生事项记录。在事项记录中记录的是：将要传送的使用通行证的使用通行证标识符；原始设备在使用通行证传送过程中的角色，亦即“目标”（在图 24 中，以缩写的形式显示为“D”）；在参考数字 24021 中接收的屏蔽使用通行证中包括的 UR_s；以及开始设备的限定存储器中的使用通行证地点（记录源地址）。

过程 BT 3. 4. 3：产生会话密钥 K_s[P]m，其中“m”是指，会话密钥是在 BT 连接阶段之后的第 m 个 BT IP 传送阶段产生的。

过程 BT 3.4.4：加密在过程 BT 3.4.3 期间产生的 K_s[P]m。加密使用在紧接着以前的使用通行证传送的执行期间产生的会话密钥 K_s[P]m－1，以及由开始设备产生的最新会话密钥 K_s[I]n。密钥 K_s[I]n 在每次执行 BT 传送阶段时生成，并且意味着传送过程在 BT 连接阶段完成之后已重复了“n”次。BT 传送阶段已经由图 23 在上文中说明。如果没有使用通行证已从原始设备传送到开始设备，则在 BT 连接阶段共享的第零阶会话密钥 K_s[I]0 将用作 K_s[I]n。获得的数据将会是 E（K_s[I]n，E（K_s[P]m－1，K_s[P]m））。

【0171】

当原始设备在执行过程 BT 3.4.1 至 3.4.4 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取原始设备会话密钥 BT 传送指令 24040。原始设备在接收到所述指令之后，将在过程 BT 3.4.4 期间产生的数据传输到主机模块，如参考数字 24041 所指示的那样。

主机模块 110 在接收到 E（K_s[I]n，E（K_s[P]m－1，K_s[P]m））之后，向开始设备发布提出原始设备会话密钥 BT 传送指令 24050，然后向其传输接收的数据（见参考数字 24051）。

【0172】

开始设备在接收到 E（K_s[I]n，E（K_s[P]m－1，K_s[P]m））之后，执行参考数字 24052 中显示的以下两个过程：

过程 BT 3.5.1：通过使用 K_s[I]n 和 K_s[P]m－1 来解密接收的数据。两组密钥数据均如对过程 BT 3.2.1 和 3.4.4 说明的那样。

过程 BT 3.5.2：检查 K_s[P]m 是否以恰当的形式包括在过程 BT 3.5.1 中获得的数据中。检查方法与对过程 UT 1.3.3 说明的方法相同。

【0173】

当开始设备在执行过程 BT 3.5.1 和 3.5.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布加密使用通行证复制、加密使用通行证移动或加密使用通行证播放指令 24060。在 BT 方式下，如 UT 方式下那样，指令的发布假定所有的需要的信息都是预定的。更加具体地，预定的信息是指，例如，在指令接收完成之后，什么 UR_s 被分

配给将要传输的使用通行证，并且在复制或回放之后会留在原始设备中的使用通行证的 UR_s 信息要被以什么形式改变。在如此接收指令之后，开始设备执行参考数字 24061 中显示的以下两个过程：

过程 BT 3.6.1：在模块 1103 中，从在过程 BT 3.1.1 中向使用通行证缓冲器发送的使用通行证中生成将要向原始设备传输的使用通行证。诸如 UPID 和 K_c 之类的信息通常是复制原样的，而只有 UR_s 以预定形式改变。

过程 BT 3.6.2：指示对于过程 BT 3.6.1 中生成的使用通行证已接收的指令是加密使用通行证复制、加密使用通行证移动还是加密使用通行证播放的标识符信息行为指示器，以及用于使用通行证||行为指示器的校验和，被计算并连接在一起。在连接之后，使用 K_s[P]m 和 *KP_d[P]加密获得的数据。亦即，用对称密钥双重加密数据。获得的数据是 E(*KP_d[P], E(K_s[P]m, 使用通行证||行为指示器||校验和))。校验和的计算如对过程 UT 2.4.2 说明的那样。

【0174】

当开始设备在执行过程 BT 3.6.1 和 3.6.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取使用通行证指令 24070。在接收到这个指令之后，开始设备执行参考数字 24071 中显示的以下过程：

过程 BT 3.7.1：如预定的那样改变使用通行证缓冲器中的使用通行证的 UR_s。在这之后，在它在限定存储器中初始记录的地方重写使用通行证。如果指令 24060 是加密使用通行证移动，则将有效性指示器标记的值设置为“无效”。

【0175】

开始设备在完成过程 BT 3.7.1 之后，将在所述过程期间已产生的数据传输到主机模块，如参考数字 24072 所指示的那样。

主机模块 110 在接收到 E（*KP_d[P]，E（K_s[P]m，使用通行证||行为指示器||校验和））之后，向原始设备发布提出使用通行证指令 24080，并且将 E（*KP_d[P]，E（K_s[P]m，使用通行证||行为指示器||

校验和））传输到设备（见参考数字 24081）。

【0176】

原始设备在接收到上述指令和数据之后，执行参考数字 24082 中显示的以下两个过程：

过程 BT 3. 8. 1：用*K_d[P]和 K_s[P]m 解密接收的数据，其中，*K_d[P]是在过程 BT 1. 7. 1 中获得的对称密钥，而 K_s[P]m 则是设备自身在过程 BT 3. 4. 3 中生成的会话密钥。

过程 BT 3. 8. 2：检查使用通行证||行为指示器||校验和是否以恰当的形式包括在过程 BT 3. 8. 1 中获得的数据中。通过检验校验和并使用对过程 UT 1. 3. 3 说明的方法来进行检查。使用校验和的检验方法如对过程 UT 2. 4. 2 说明的那样。

【0177】

在上述之后，主机模块 110 可以向原始设备发布检查执行状态指令 24090，以便确认通过开始设备的使用通行证的接收是否已获致正常结束。执行状态被作为响应 24091 从原始设备传输到主机模块。

重复上述 BT 传送阶段使得可以连续地执行使用通行证传送而不用重复连接阶段。

【0178】

（BT 方式下的设备间相互再认证处理顺序）

在原始设备和开始设备之间的一次 BT 连接阶段的执行已继之以各个对称设备公共密钥 KP_d[P]和 KP_s[I]及第零阶会话密钥 K_s[P]0 和 K_s[I]0 之间的共享而且还有这些密钥中的每一个在连接记录中的记录之后，如果记录器/播放器变得异常，并且会话密钥在使用通行证传输模块和接收模块两者中丢失，则相互认证能够在与连接阶段相比的小的处理负荷下重新完成。这个相互再认证处理顺序将使用图 25 来说明。BT 方式下的这个处理阶段在下文中被称作“BT 再连接阶段”。

【0179】

首先，假定以下给出说明：在参考数字 25000 中的 BT 连接阶段

完成之后，由于异常的发生而在原始设备和开始设备之间造成断开，因此，在那个时间点的最新会话密钥 K_s[P]m 与 K_s[I]n 和/或对称设备公共密钥*KP_s[P]与*KP_d[I]在两个设备中丢失，如参考数字 25001 所指示的那样。

在上述情况下，主机模块 110 首先向原始设备发布产生原始设备会话密钥 BT 再连接指令 25010。

原始设备在接收到所述指令之后，执行参考数字 25011 中显示的以下两个过程：

过程 BT 4.1.1：产生第零阶会话密钥 K_s[P]0'。

过程 BT 4.1.2：加密在过程 BT 4.1.1 期间产生的 K_s[P]0'。加密使用设备的固有连接记录中记录的会话密钥 K_s[I]CL 和设备公共密钥 KP_d[I]CL。密钥 K_s[I]CL 和 KP_d[I]CL 指示密钥数据记录在连接记录中。最终获得的数据是 E（KP_d[I]CL，E（K_s[I]CL，K_s[P]0'））。

【0180】

当原始设备在执行过程 BT 4.1.1 和 4.1.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取原始设备会话密钥 BT 再连接指令 25020。原始设备在接收到所述指令之后，将上述数据 E（KP_d[I]CL，E（K_s[I]CL，K_s[P]0'））传输到主机模块。主机模块 110 在接收到 E（KP_d[I]CL，E（K_s[I]CL，K_s[P]0'））之后，向开始设备发布提出原始设备会话密钥 BT 再连接指令 25030，然后向其传输接收的数据（见参考数字 25031）。开始设备在接收到 E（KP_d[I]CL，E（K_s[I]CL，K_s[P]0'））之后，执行参考数字 25032 中显示的以下两个过程：

过程 BT 4.2.1：解密接收的数据。解密使用设备的固有保护信息区域中嵌入的 K_d[I]和连接记录中包括的会话密钥 K_s[I]CL。

过程 BT 4.2.2：检查 K_s[P]0'是否以恰当的形式包括在过程 BT 4.2.1 的执行结果中。检查方法与对过程 UT 1.3.3 说明的方法相同。

【0181】

在过程 BT 4.2.1 和 4.2.2 的执行期间，主机模块估计处理的完成时刻，并且在适当的时刻发布获取开始设备会话密钥 BT 再连接指令 25040。开始设备在接收到所述指令之后，执行参考数字 25041 中显示的以下 3 个过程：

过程 BT 4.3.1：产生第零阶会话密钥 K_s[I]0'。

过程 BT 4.3.2：加密在过程 BT 4.3.1 期间产生的 K_s[I]0'。加密使用设备的固有连接记录中记录的会话密钥 K_s[P]CL 和设备公共密钥 KP_d[P]CL。密钥 K_s[P]CL 和 KP_d[P]CL 指示密钥数据记录在连接记录中。最终获得的数据是 E（KP_d[P]CL，E（K_s[P]CL，K_s[I]0'））。

过程 BT 4.3.3：通过重写在连接记录中记录在过程 BT 4.2.2 期间接收的 K_s[P]0'和在过程 BT 4.3.1 期间产生的 K_s[I]0'两者。在那时，KP_d[P]和 TM_[P]维持不变。

【0182】

开始设备在完成过程 BT 4.3.3 之后，将在过程 BT 4.3.2 期间产生的数据 E（KP_d[P]CL，E（K_s[P]CL，K_s[I]0'））传输到主机模块，如参考数字 25042 所指示的那样。主机模块 110 在接收到 E（KP_d[P]CL，E（K_s[P]CL，K_s[I]0'））之后，向原始设备发布提出开始设备会话密钥 BT 再连接指令 25050，然后向其传输接收的数据（见参考数字 25051）。原始设备在接收到 E（KP_d[P]CL，E（K_s[P]CL，K_s[I]0'））之后，执行参考数字 25052 中显示的以下 3 个过程：

过程 BT 4.4.1：解密接收的数据。解密使用设备的固有保护信息区域中嵌入的 K_d[P]和连接记录中包括的会话密钥 K_s[P]CL。

过程 BT 4.4.2：检查 K_s[I]0'是否以恰当的形式包括在过程 BT 4.4.1 的执行结果中。检查方法与对过程 UT 1.3.3 说明的方法相同。

过程 BT 4.4.3：通过重写在连接记录中记录在过程 BT 4.4.2 期间接收的 K_s[I]0'和在过程 BT 4.1.1 期间产生的 K_s[P]0'两者。在那时，KP_d[I]和 TM_[I]维持不变。

【0183】

当过程 BT 4.4.3 完成时，这就表明*KP_d[I]（与*K_d[I]相同）、K_s[P]0'和 K_s[I]0'之间的共享已完成。当在上述过程完成之后执行 BT

PI 传送阶段时，密钥 K_s[I]0'用作 K_s[I]n－1。当在上述过程完成之后执行 BT IP 传送阶段时，密钥 K_s[P]0'用作 K_s[P]m－1。

【0184】

（关于 BT PI 传送阶段的使用通行证恢复处理顺序）

如果在使用通行证在 BT PI 传送阶段的移动期间，记录器/播放器变得异常，并且在被传送的使用通行证在原始设备和开始设备两者中丢失，则以这样的形式恢复使用通行证以存在于原始设备中：使用通行证具有与它初始具有的相同的 UR_s。这样的使用通行证恢复处理将使用图 26 来说明。BT 方式下的这个处理阶段在下文中被称作“BT PI 恢复阶段”。

【0185】

首先，假定以下给出说明：在 BT PI 传送阶段期间，开始设备在接收提出使用通行证指令 26010 及其后的使用通行证 26011。说明还假定：在使用通行证接收处理被执行到完成之前，由于异常的发生而在原始设备和开始设备之间造成断开，因此，用于加密流动的使用通行证 26011 的会话密钥 K_s[I]n 和*KP_d[I]（*K_d[I]）在两个设备中丢失（见参考数字 26020）。在这样的情况下，首先，执行在上文中说明的 BT 再连接阶段，并且重新共享*KP_d[P]（与*K_d[P]相同）、*KP_d[I]（与*K_d[I]相同）、K_s[P]0'和 K_s[I]0'。

【0186】

在完成 BT 再连接阶段之后，主机模块 110 首先向原始设备发布搜索事项记录 BT 恢复指令 26030。下一步在发布所述指令之后，如参考数字 26031 所指示的那样，主机模块发送在被传输的使用通行证 21011 的使用通行证标识符。原始设备在接收到标识符之后，执行参考数字 26032 中显示的以下过程：

过程 BT 5.1.1：为了包含与所述标识符相同的标识符值的事项记录而搜索保护信息区域。

【0187】

当原始设备在执行过程 BT 5.1.1 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取使用通行证地点指令 26040。原始设备

在接收到所述指令之后，将在过程 BT 5.1.1 期间检测到的事项记录中记录的使用通行证地点信息传输到主机模块，如参考数字 26041 所示。

主机模块 110 在接收到使用通行证地点信息之后，向开始设备发布搜索使用通行证恢复指令 26050，然后向其发送接收的数据（见参考数字 26051）。

【0188】

开始设备在接收到使用通行证地点信息之后，执行参考数字 26052 中显示的以下 3 个过程：

过程 BT 5.2.1：为了由接收的使用通行证地点指定的使用通行证存储区域而搜索限定存储器。

过程 BT 5.2.2：检查过程 BT 5.2.1 期间检测到的使用通行证的有效性指示器标记的值，并且在使用通行证状态中设立值“有效”、“无效”或“未记录”。

过程 BT 5.2.3：生成用于 BT 方式的事项状态。事项状态是“将要恢复的使用通行证的 UPID||在过程 BT 5.2.1 期间检测到的使用通行证的 UR_s||过程 BT 5.2.2 期间设立的使用通行证状态||26041 中接收到的使用通行证地点||散列值”。从 K_s[P]m||K_s[I]n||UPID||UR_s||使用通行证状态||使用通行证地点中计算散列值。这里使用的 K_s[P]m||K_s[I]n 是当连接阶段或再连接阶段完成时共享的最新会话密钥。这些密钥指示，在所述阶段之后，BT PI 传送阶段和 BT IP 传送阶段已分别执行了“m”次和“n”次。这个过程期间生成的事项状态在下文中被称作“BT PI 传送状态”。

【0189】

当开始设备在执行过程 BT 5.2.1 至 5.2.3 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取事项状态 BT 恢复指令 26060。开始设备在接收到所述指令之后，将在过程 BT 5.2.3 期间生成的 BT PI 事项状态传输到主机模块，如参考数字 26061 所示。

主机模块 110 在接收到 BT PI 事项状态之后，向原始设备发布检

验事项状态 BT PI 恢复指令 26070，然后向其发送接收的 BT PI 事项状态（见参考数字 26071）。

原始设备在接收到 BT PI 事项状态之后，执行参考数字 26072 中显示的以下两个过程：

过程 BT 5.3.1：检验 BT PI 事项状态，并且确认 BT PI 事项状态中包括的使用通行证标识符、使用通行证状态和使用通行证地点。通过从设备自身保持的 K_s[P]m 并且从 K_s[I]n 中计算数据包含的散列值，完成 BT PI 事项状态的检验。如果计算结果匹配散列值，则判断数据未被伪造。同样，使用通行证标识符用于确认使用通行证是否是要被恢复的，使用通行证状态用于判断恢复是否是可能的，而使用通行证地点则用于确认，设备的固有区域中记录的使用通行证地点所指定的限定存储器中的使用通行证存储区域是否已被恰当地搜索。如果使用通行证状态是“无效”或“未记录”，则用于使用通行证的恢复处理在原始设备中执行。然而，如果使用通行证状态不同于设备的固有事项记录中记录的信息，则不执行使用通行证恢复处理。

过程 BT 5.3.2：执行使用通行证恢复处理。通过以下完成使用通行证的恢复：将预期使用通行证的有效性指示器标记变为“有效”（如果“无效”的话），并且用事项记录中记录的使用通行证重写这个使用通行证。

当过程 BT 5.3.2 完成时，在传输之前存在的使用通行证将会存在于原始设备中。

【0190】

（关于 BT IP 传送阶段的使用通行证恢复处理顺序）

如果在使用通行证在 BT IP 传送阶段的移动期间，记录器/播放器变得异常，并且在被传送的使用通行证在原始设备和开始设备两者中丢失，则能够以这样的形式恢复使用通行证以存在于开始设备中：使用通行证具有与它初始具有的相同的 UR_s。这样的使用通行证恢复处理将使用图 27 来说明。BT 方式下的这个处理阶段在下文中被称作“BT

IP 恢复阶段”。

【0191】

首先，假定以下给出说明：在 BT IP 传送阶段期间，原始设备在接收提出使用通行证指令 27010 及其后的使用通行证 27011。说明还假定：在使用通行证接收处理被执行到完成之前，由于异常的发生而在原始设备和开始设备之间造成断开，因此，用于加密流动的使用通行证 27011 的会话密钥 K_s[P]n 和*KP_d[P]（*K_d[P]）在两个设备中丢失（见参考数字 27020）。在这样的情况下，首先，执行在上文中说明的 BT 再连接阶段，并且重新共享*KP_d[P]（与*K_d[P]相同）、*KP_d[I]（与*K_d[I]相同）、K_s[P]0’和 K_s[I]0’。

【0192】

在完成 BT 再连接阶段之后，主机模块首先向原始设备发布搜索事项记录 BT 恢复指令 27030。下一步在发布所述指令之后，如参考数字 27031 所指示的那样，主机模块发送在被传输的使用通行证 27011 的使用通行证标识符。原始设备在接收到标识符之后，执行参考数字 27032 中显示的以下过程：

过程 BT 6.1.1：为了包含与所述标识符相同的标识符值的事项记录而搜索保护信息区域。

【0193】

当原始设备在执行过程 BT 6.1.1 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取使用通行证地点指令 27040。原始设备在接收到所述指令之后，将在过程 BT 6.1.1 期间检测到的事项记录中记录的使用通行证地点信息传输到主机模块，如参考数字 27041 所示。

主机模块 110 在接收到使用通行证地点信息之后，向开始设备发布搜索使用通行证恢复指令 27050，然后向其发送接收的数据（见参考数字 27051）。

【0194】

开始设备在接收到使用通行证地点信息之后，执行参考数字 27052 中显示的以下 3 个过程：

过程 BT 6.2.1：为了由接收的使用通行证地点指定的使用通行证存储区域而搜索限定存储器。

过程 BT 6.2.2：检查过程 BT 6.2.1 期间检测到的使用通行证的有效性指示器标记的值，并且在使用通行证状态中设立值“有效”、“无效”或“未记录”。

过程 BT 6.2.3：生成用于 BT 方式的事项状态。事项状态是“将要恢复的使用通行证的 UPID||在过程 BT 6.2.1 期间检测到的使用通行证的 UR_s||过程 BT 6.2.2 期间设立的使用通行证状态||27041 中接收到的使用通行证地点||散列值”。从 K_s[P]m||K_s[I]n－1||UPID||UR_s||使用通行证状态||使用通行证地点中计算散列值。这里使用的 K_s[P]m||K_s[I]n－1 是当连接阶段或再连接阶段完成时共享的最新会话密钥。这些密钥指示，在所述阶段之后，BT PI 传送阶段和 BT IP 传送阶段已分别执行了“m”次和“n－1”次。这个过程期间生成的事项状态在下文中被称作“BT IP 传送状态”。

【0195】

当开始设备在执行过程 BT 6.2.1 至 6.2.3 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取事项状态 BT 恢复指令 27060。开始设备在接收到所述指令之后，将在过程 BT 6.2.3 期间生成的 BT IP 事项状态传输到主机模块，如参考数字 27061 所示。

主机模块 110 在接收到 BT IP 事项状态之后，向原始设备发布检验事项状态 BT IP 恢复指令 27070，然后向其发送接收的 BT IP 事项状态（见参考数字 27071）。

【0196】

原始设备在接收到 BT IP 事项状态之后，执行参考数字 27072 中显示的以下过程：

过程 BT 6.3.1：检验 BT IP 事项状态，并且确认 BT IP 事项状态中包括的使用通行证标识符、使用通行证状态和使用通行证地点。通过从设备自身保持的 K_s[P]m 并且从 K_s[I]n－1 中计算数据包含的散列值，完成 BT IP 事项状态的检验。如果计算结果匹配散列值，则判断

数据未被伪造。同样，使用通行证标识符用于确认使用通行证是否是要被恢复的，UR_s 和使用通行证状态用于判断恢复是否是可能的，而使用通行证地点则用于确认，设备的固有区域中记录的使用通行证地点所指定的限定存储器中的使用通行证存储区域是否已被恰当地搜索。使用通行证状态可能是“无效”，或者，在 BT IP 传送状态中包括的 UR_s 已核对过程 BT 6.1.1 期间检测到的事项记录中记录的使用通行证的 UR_s 之后，开始设备中留下的预期使用通行证的 UR_s 可能发现已被改变。在这样的情况下，对随后的使用通行证执行恢复处理。

【0197】

当原始设备在执行过程 BT 6.3.1 时，主机模块 110 并行地发布产生开始设备会话密钥 BT 传送指令 27080。开始设备在接收到所述指令之后，执行参考数字 27081 中显示的以下两个过程：

过程 BT 6.4.1：产生会话密钥 K_s[I]n，其中“n”是指，这个过程是 BT 连接阶段完成之后的第 n 个 BT IP 传送阶段。

过程 BT 6.4.2：加密在过程 BT 6.4.1 期间产生的 K_s[I]n。加密使用紧接着以前的使用通行证传送的执行期间产生的会话密钥 K_s[I]n－1，以及由开始设备产生的最新会话密钥 K_s[P]m。密钥 K_s[P]m 是指，在 BT 连接阶段完成之后，BT IP 传送阶段已重复了“m”次。如果没有使用通行证已从开始设备传送到原始设备，则在 BT 连接阶段共享的第零阶会话密钥 K_s[P]0’将用作 K_s[P]m。获得的数据将会是 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））。

【0198】

当开始设备在执行过程 BT 6.4.1 和 6.4.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取开始设备会话密钥 BT 传送指令 27090。开始设备在接收到所述指令之后，将在过程 BT 6.4.2 期间产生的数据 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））传输到主机模块，如参考数字 27091 所示。

主机模块 110 在接收到 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n））之后，向原始设备发布提出开始设备会话密钥 BT 传送指令 27100，然

后向其传输接收的数据（见参考数字 27101）。

【0199】

原始设备接收 E（K_s[P]m，E（K_s[I]n－1，K_s[I]n）），并且如果在过程 BT 6.3.1 中，开始设备中的使用通行证发现需要恢复，则原始设备执行参考数字 27102 中显示的以下两个过程：

过程 BT 6.5.1：通过使用 K_s[P]m 和 K_s[I]n－1 解密接收的数据。两组密钥数据均如对过程 BT 6.2.3 说明的那样。

过程 BT 6.5.2：检查 K_s[I]n 是否以恰当的形式包括在过程 BT 6.5.1 中获得的数据中。检查方法与对过程 UT 1.3.3 说明的方法相同。

【0200】

当原始设备在执行过程 BT 6.5.1 和 6.5.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布加密使用通行证恢复指令 27110。原始设备在接收到所述指令之后，执行参考数字 27111 中显示的以下两个过程：

过程 BT 6.6.1：连接在过程 BT 6.2.1 期间检测到的事项记录中记录的 UPID 和 UR_s，并且将连接的数据传输到使用通行证传输模块 1301。

过程 BT 6.6.2：计算与过程 BT 6.6.1 期间的使用通行证传输模块 1301 中设立的 UPID||UR_s 相关联的校验和，然后将校验和连接到接收的数据，并且使用 K_s[I]n 和*KP_d[I]加密获得的数据。亦即，用对称密钥进行双重加密。获得的数据是 E（*KP_d[I]，E（K_s[I]n，UPID||UR_s||校验和））。校验和的计算如对过程 UT 2.4.2 说明的那样。

【0201】

当原始设备在执行过程 BT 6.6.1 和 6.6.2 时，主机模块估计处理的完成时刻，并且在适当的时刻发布获取恢复使用通行证指令 27120。原始设备在接收到所述指令之后，将 E（*KP_d[I]，E（K_s[I]n，UPID||UR_s||校验和））传输到主机模块（见参考数字 27121）。

主机模块 110 在接收到 E（*KP_d[I]，E（K_s[I]n，UPID||UR_s||

校验和））之后，向开始设备发布恢复使用通行证指令 27130，然后传输 E（*KP_d[I]，E（K_s[I]n，UPID||UR_s||校验和））和数据写入目标使用通行证地点（见参考数字 27131）。

【0202】

开始设备在接收到上述指令和数据之后，执行参考数字 27132 中显示的以下 4 个过程：

过程 BT 6.7.1：用*K_d[I]和 K_s[I]n 解密接收的数据 E(*KP_d[I]，E（K_s[I]n，UPID||UR_s||校验和）），其中，*K_d[I]是在再连接阶段 27021 期间获得的对称密钥，而 K_s[I]n 则是设备自身在过程 BT 6.4.1 期间产生的会话密钥。

过程 BT 6.7.2：检查 UPID||UR_s||校验和是否以恰当的形式包括在过程 BT 6.7.1 中获得的数据中。通过检验校验和并使用对过程 UT 1.3.3 说明的方法来进行检查。使用校验和的检验方法如对过程 UT 2.4.2 说明的那样。

过程 BT 6.7.3：从接收的使用通行证地点所指定的限定存储器的使用通行证存储区域中读出使用通行证，进入到使用通行证缓冲器中，并且检查使用通行证的 UPID 是否与过程 BT 6.7.2 中的通过解密获得的 UPID 相一致。如果两个 UPID 不一致，则中止处理。

过程 BT 6.7.4：在限定存储器中记录接收的使用通行证。在使用通行证的记录期间，将有效性指示器标记设置为“有效”。

【0203】

在上述之后，主机模块可以向开始设备发布检查执行状态指令 27140，以便确认开始设备已恰当地完成在限定存储器中记录使用通行证。执行状态被作为响应 27141 从开始设备传输到主机模块。当过程 BT 6.7.2 完成时，在传输之前存在的使用通行证将会存在于开始设备中。

【0204】

尽管上面已说明了优选实施例，但是本发明并不限于优选实施例。另外，本发明可以容许实施例的各种方式，并且同样可应用于其他设备和系统。

例如，已用在优选实施例的说明中的指令、模块以及其他的指示仅仅是一个例子，并且不限于上述实施例。例如，上述实施例中的使用通行证可以被称作许可信息或机密信息。

【参考数字解释】

100：网络接口，101：保护信息区域，102：记录模块，103：回放模块，105：用户接口网桥，106、107：外部存储器接口，108：处理器，110：主机模块，111：主机安全管理器，112：记录器/播放器，150：分发服务器，125、126、240：磁盘驱动器，221：使用通行证传送模块，222：限定存储控制器，223：限定存储器，231：处理器

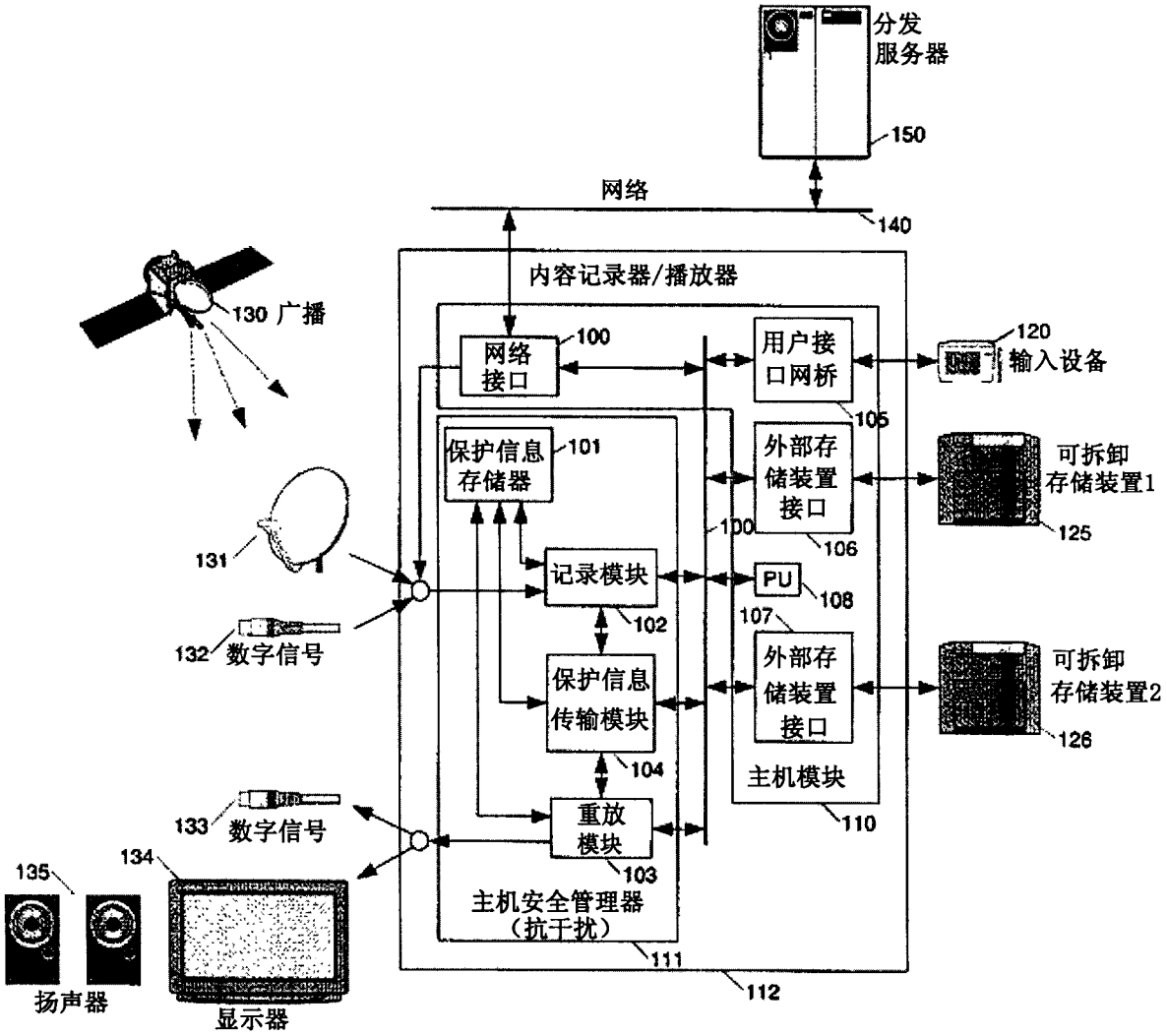

分发
服务器
150
网络
140
内容记录器/播放器
130 广播
网络
接口
100
用户接
口网桥
105
120
输入设备
保护信息
存储器
101
外部存
储装置
接口
106
可拆卸
存储装置1
125
131
记录模块
102
PU
108
107
132 数字信号
保护信息
传输模块
104
外部存
储装置
接口
可拆卸
存储装置2
126
主机模块
110
133 数字信号
重放
模块
103
134
135
主机安全管理器
（抗干扰）
111
112
扬声器
显示器

图1

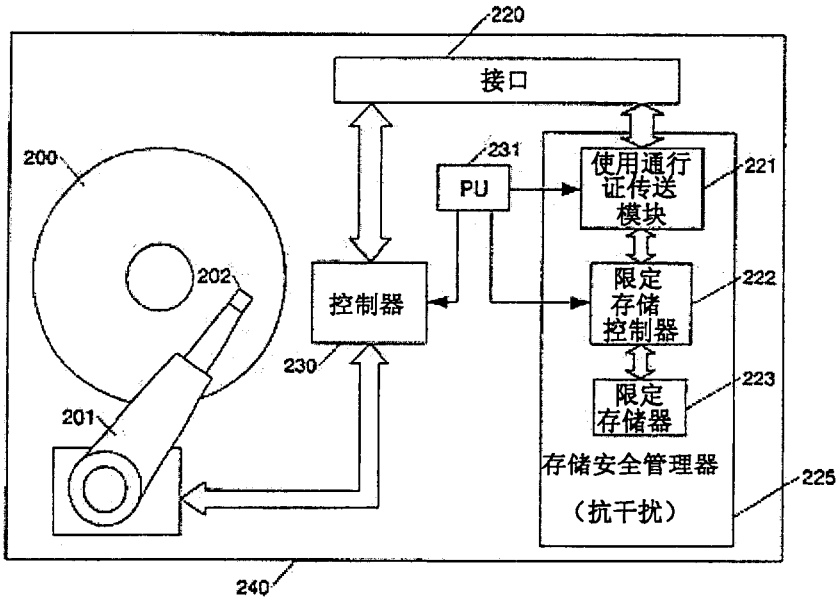

220
接口
231
PU
使用通行证传送模块
221
200
202
控制器
222
限定存储控制器
230
223
限定存储器
201
存储安全管理器
（抗干扰）
225
240

图2

符号	名称	密钥属性	特征与特性
A‖B	数据连接	-	数据A和数据B的连接
E(X,Y)	加密	-	用数据X加密数据Y的算术运算。如果X是公共密钥数据，则加密是公共密钥加密，而如果X是对称密钥数据，则加密是对称密钥加密。
D(X,Y)	解密	-	用数据X解密数据Y的算术运算。如果X是私有密钥数据，则用私有密钥解密用公共密钥加密的数据，而如果X是对称密钥数据，则用对称密钥解密用对称密钥加密的数据。
H(X)	散列值计算	-	计算数据X的散列值的算术运算
DCC	设备类别证书	-	指示KPdc的有效性的证书。包括KCA加密的电子签名。
RDCL	撤销设备类别清单	-	被证书机构撤销的设备类别证书的清单。记录在保护信息存储器和使用通行证传送模块中。
RDCL.D	撤销设备类别清单的发布日期	-	撤销设备类别证书的清单中包含的信息。所述信息指示撤销设备类别证书的清单的发布日期和时间。
KP_{CA}	证书机构公共密钥	公共密钥	由证书机构发布并且嵌入在保护信息存储器中的公共密钥。用于解密设备类别证书的电子签名部分。
K_{CA}	证书机构私有密钥	私有密钥	由证书机构管理的私有密钥。用于加密设备类别证书的电子签名部分。
KP_{dc}	设备类别公共密钥	公共密钥	嵌入在保护信息存储器中的公共密钥。具有设备的固有区域中嵌入的这个密钥的设备的有效性，由包括所述密钥的设备类别证书指示。能够为多个设备嵌入所述密钥。
K_{dc}	设备类别私有密钥	私有密钥	嵌入在保护信息存储器中的私有密钥。用于解密KPdc加密的数据。
KP_d	设备公共密钥	私有密钥	嵌入在保护信息存储器中的公共密钥。为全部设备嵌入唯一的密钥。
K_d	设备私有密钥	私有密钥	嵌入在保护信息存储器中的私有密钥。用于解密KPd加密的数据。
$*KP_t$	对称设备公共密钥	对称密钥	"x"表示"dc"或"d"。这个对称密钥是在用公共密钥加密期间生成的。
$*K_t$	对称设备私有密钥	对称密钥	"x"表示"dc"或"d"。这个对称密钥是在用私有密钥加密期间生成的。取与"KPx"所取相同的值。
K_{Ch}	质询密钥	对称密钥	用于临时对称加密的对称密钥，在使用通行证传送模块中动态生成。用于为使用通行证加密而加密临时对称会话密钥。
K_s	会话密钥	对称密钥	用于临时对称加密的对称密钥，在使用通行证传送模块中动态生成。用于在使用通行证传送期间加密数据。在连接过程期间，在原始设备和开始设备之间共享第零阶会话密钥。
K_c	内容密钥	对称密钥	用于加密和解密内容。
[P]	在原始设备处的数据产生（下标）	-	是指原始设备中产生的数据。原始设备是指通过检验从其他设备发送的设备类别证书来发起连接建立过程的设备。
[I]	在开始设备处的数据产生（下标）	-	是指开始设备中产生的数据。开始设备是指通过向其他设备传输设备的固有证书来发起连接建立过程的设备。

图3

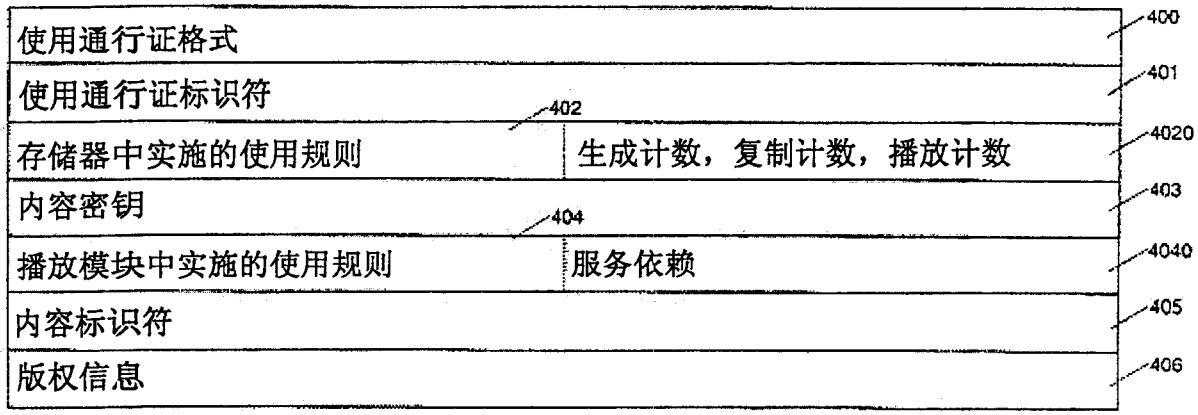

使用通行证格式
400
使用通行证标识符
401
402
存储器中实施的使用规则
生成计数，复制计数，播放计数
4020
内容密钥
403
404
播放模块中实施的使用规则
服务依赖
4040
内容标识符
405
版权信息
406

图4

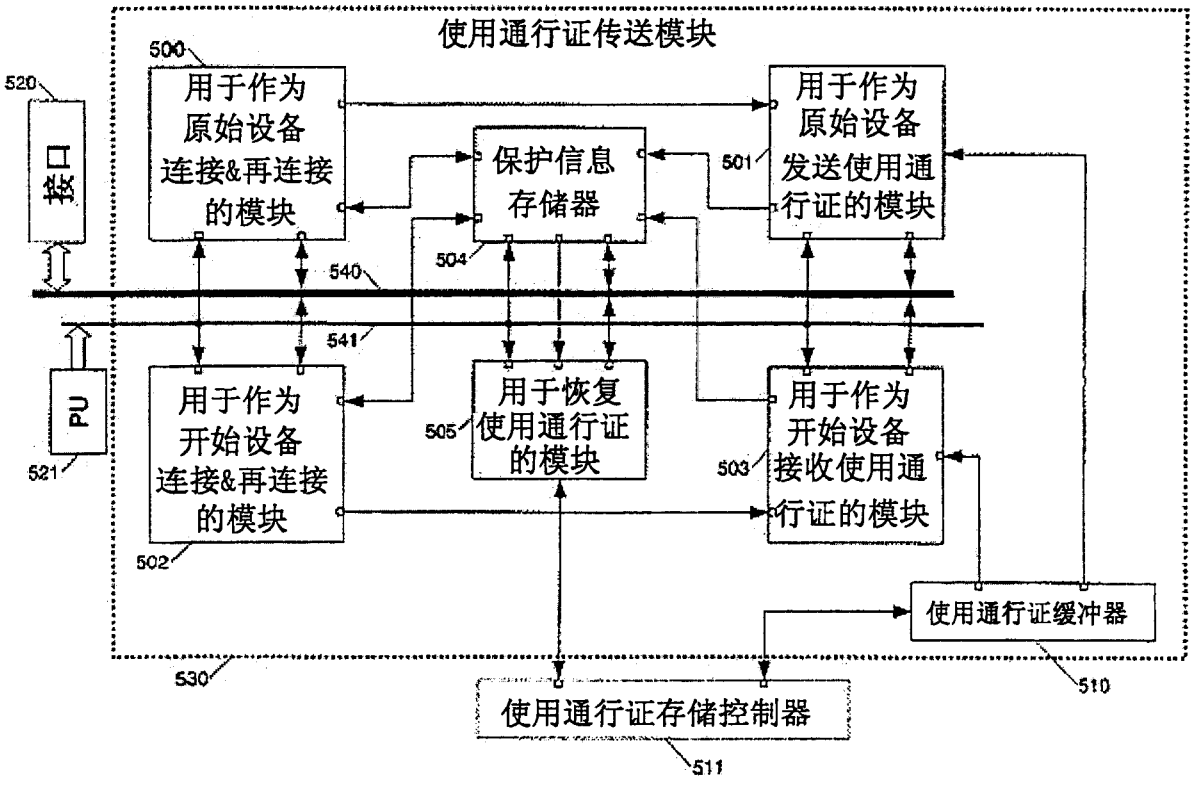

使用通行证传送模块
500
520
接口
用于作为原始设备连接&再连接的模块
保护信息存储器
501
用于作为原始设备发送使用通行证的模块
504
540
541
PU
521
用于作为开始设备连接&再连接的模块
502
505
用于恢复使用通行证的模块
503
用于作为开始设备接收使用通行证的模块
使用通行证缓冲器
510
530
使用通行证存储控制器
511

图5

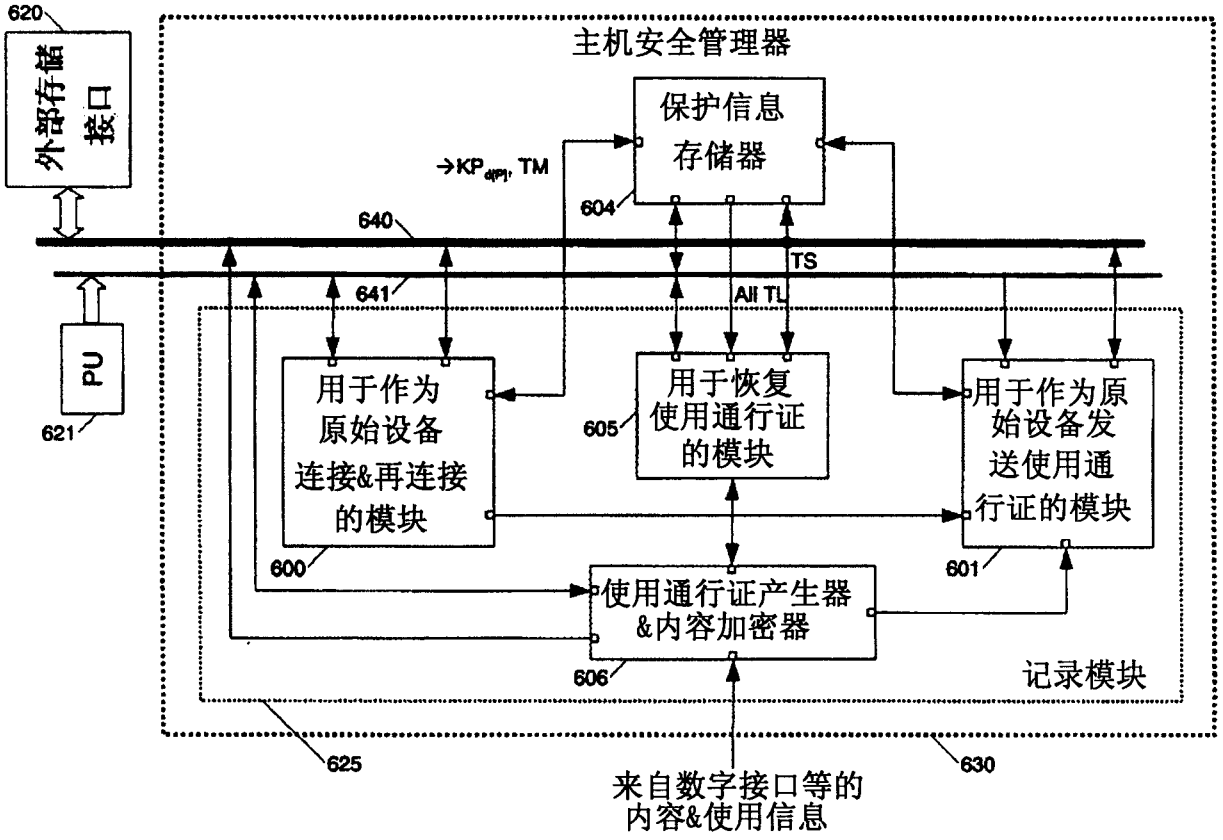

620
外部存储接口
主机安全管理器
保护信息存储器
→KP_dPI, TM
604
640
TS
641
All TL
PU
621
用于作为原始设备连接&再连接的模块
600
用于恢复使用通行证的模块
605
用于作为原始设备发送使用通行证的模块
601
使用通行证产生器&内容加密器
606
记录模块
625
630
来自数字接口等的内容&使用信息

图6

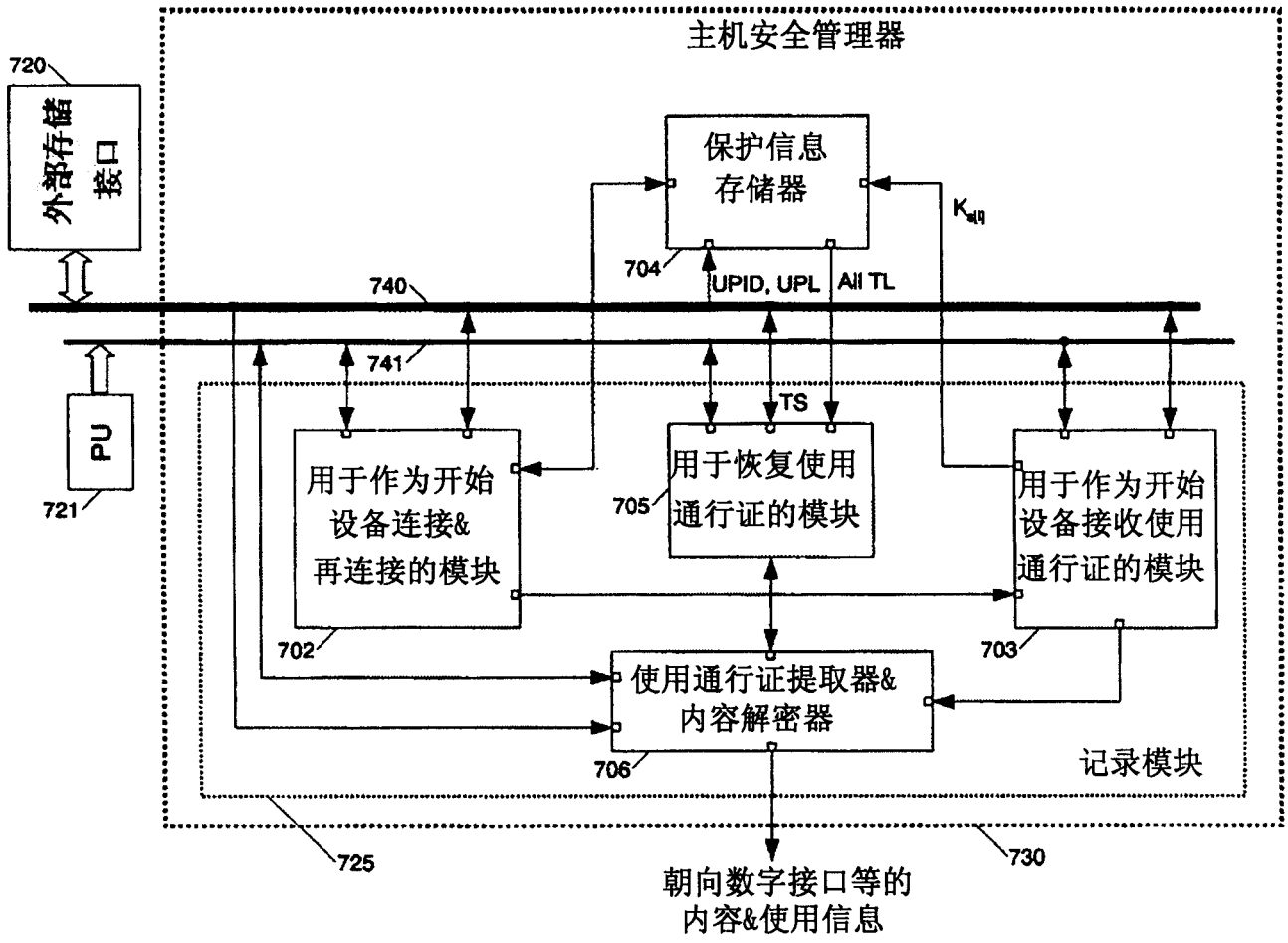

主机安全管理器
720
外部存储接口
保护信息存储器
704
UPID, UPL
All TL
740
741
PU
721
TS
用于作为开始设备连接&再连接的模块
用于恢复使用通行证的模块
705
用于作为开始设备接收使用通行证的模块
702
703
使用通行证提取器&内容解密器
706
记录模块
725
730
朝向数字接口等的内容&使用信息

图7

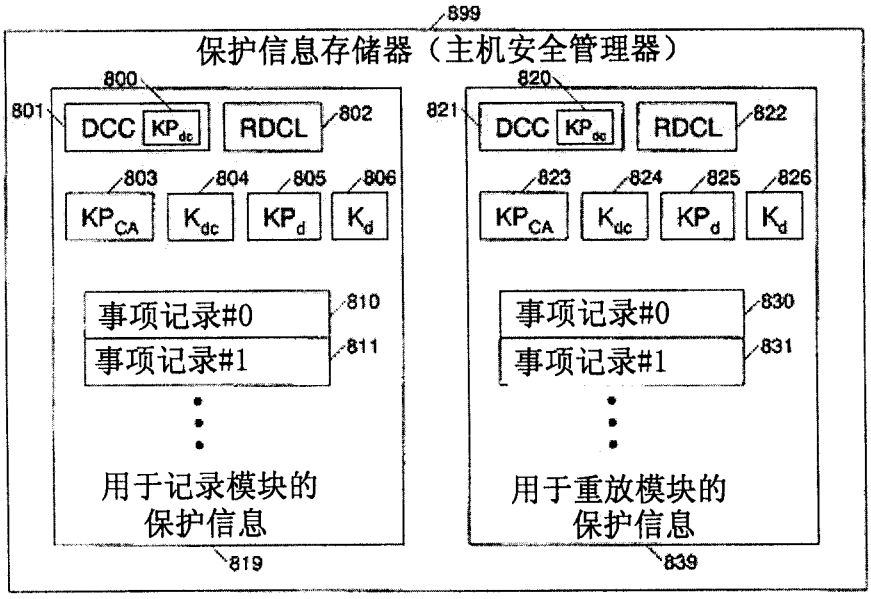

899
保护信息存储器（主机安全管理器）
800
801
DCC KPdc
RDCL
802
803
804
805
806
KPCA
Kdc
KPd
Kd
事项记录#0
事项记录#1
810
811
用于记录模块的
保护信息
819
820
821
DCC KPdc
RDCL
822
823
824
825
826
KPCA
Kdc
KPd
Kd
事项记录#0
事项记录#1
830
831
用于重放模块的
保护信息
839

图8

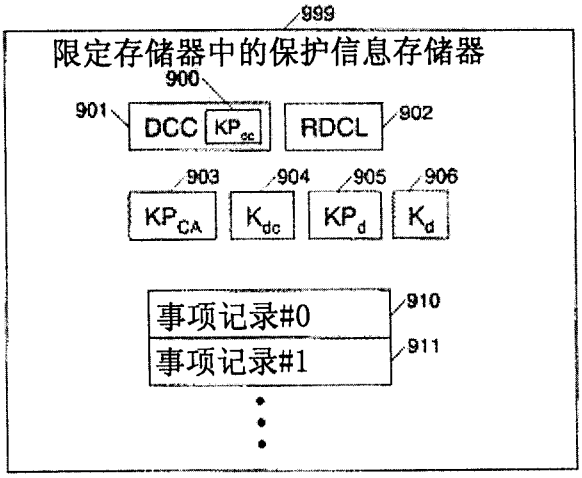

999
限定存储器中的保护信息存储器
900
901
DCC KPdc
RDCL
902
903
904
905
906
KPCA
Kdc
KPd
Kd
事项记录#0
事项记录#1
910
911

图9

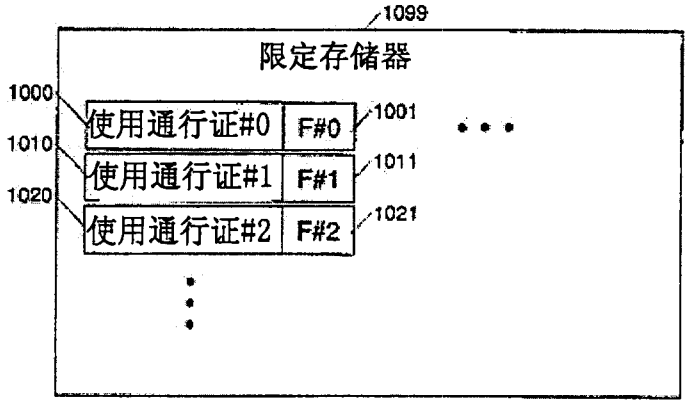

1099
限定存储器
1000
使用通行证#0
F#0
1001
1010
使用通行证#1
F#1
1011
1020
使用通行证#2
F#2
1021

图10

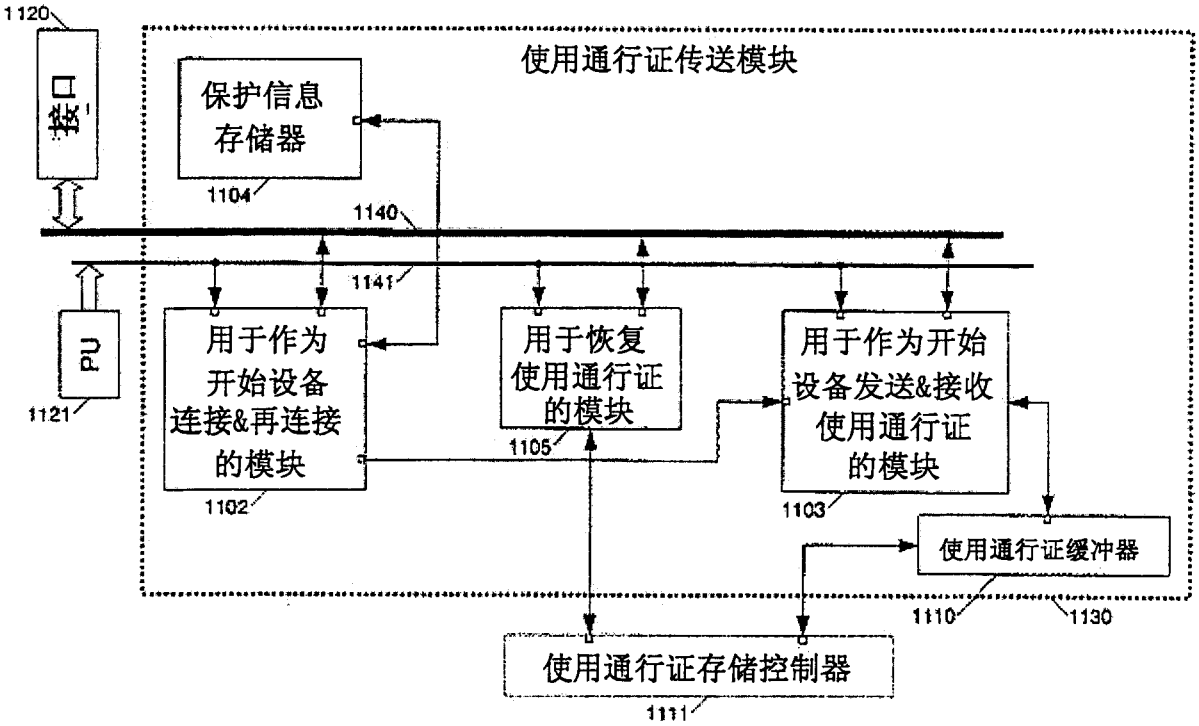

1120
接口
使用通行证传送模块
保护信息
存储器
1104
1140
1141
PU
1121
用于作为
开始设备
连接&再连接
的模块
1102
用于恢复
使用通行证
的模块
1105
用于作为开始
设备发送&接收
使用通行证
的模块
1103
使用通行证缓冲器
1110
1130
使用通行证存储控制器
1111

图11

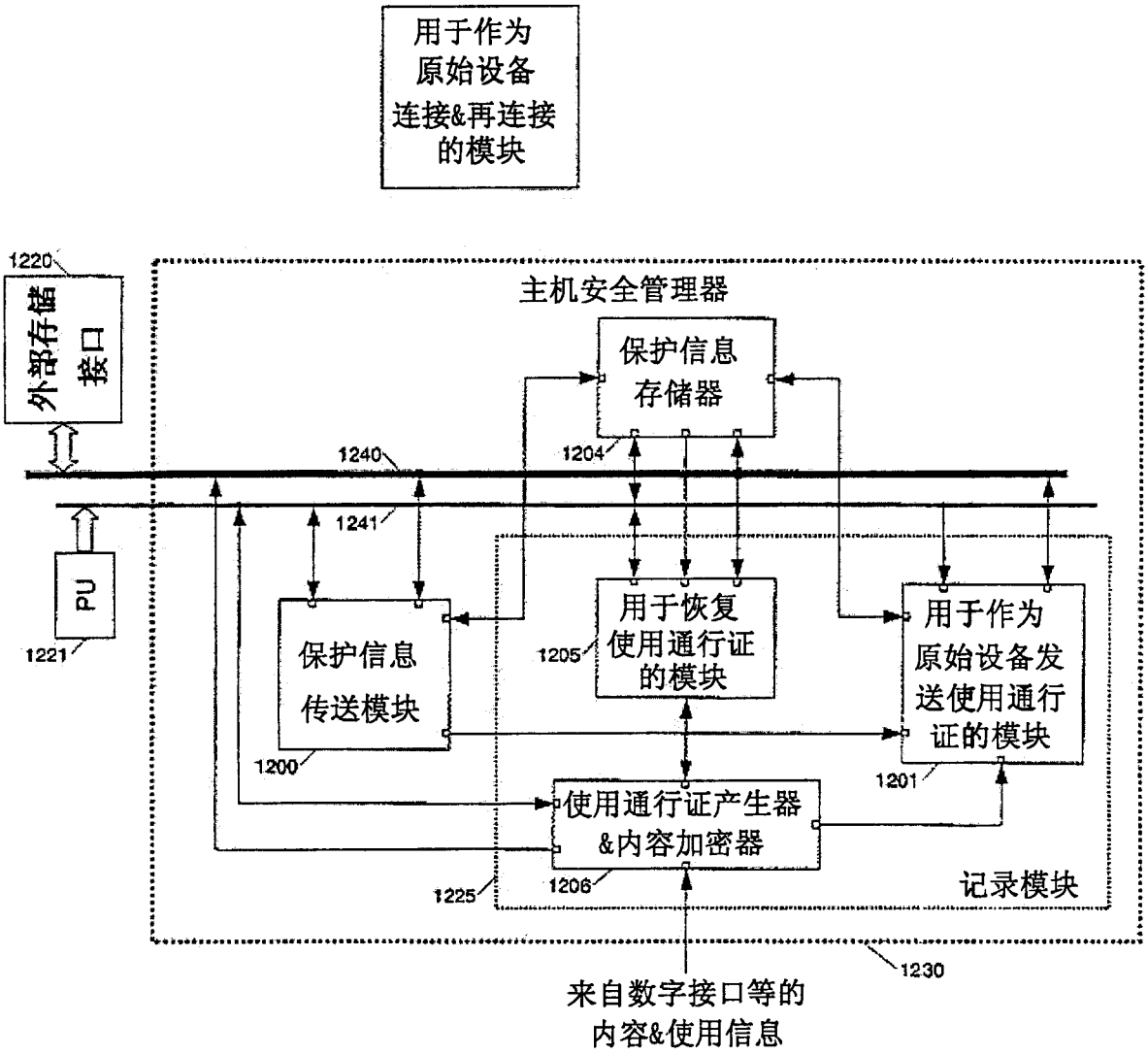

用于作为
原始设备
连接&再连接
的模块
1220
外部存储
接口
主机安全管理器
保护信息
存储器
1204
1240
1241
PU
1221
保护信息
传送模块
1200
用于恢复
使用通行证
的模块
1205
用于作为
原始设备发
送使用通行
证的模块
1201
使用通行证产生器
&内容加密器
1206
1225
记录模块
1230
来自数字接口等的
内容&使用信息

图12

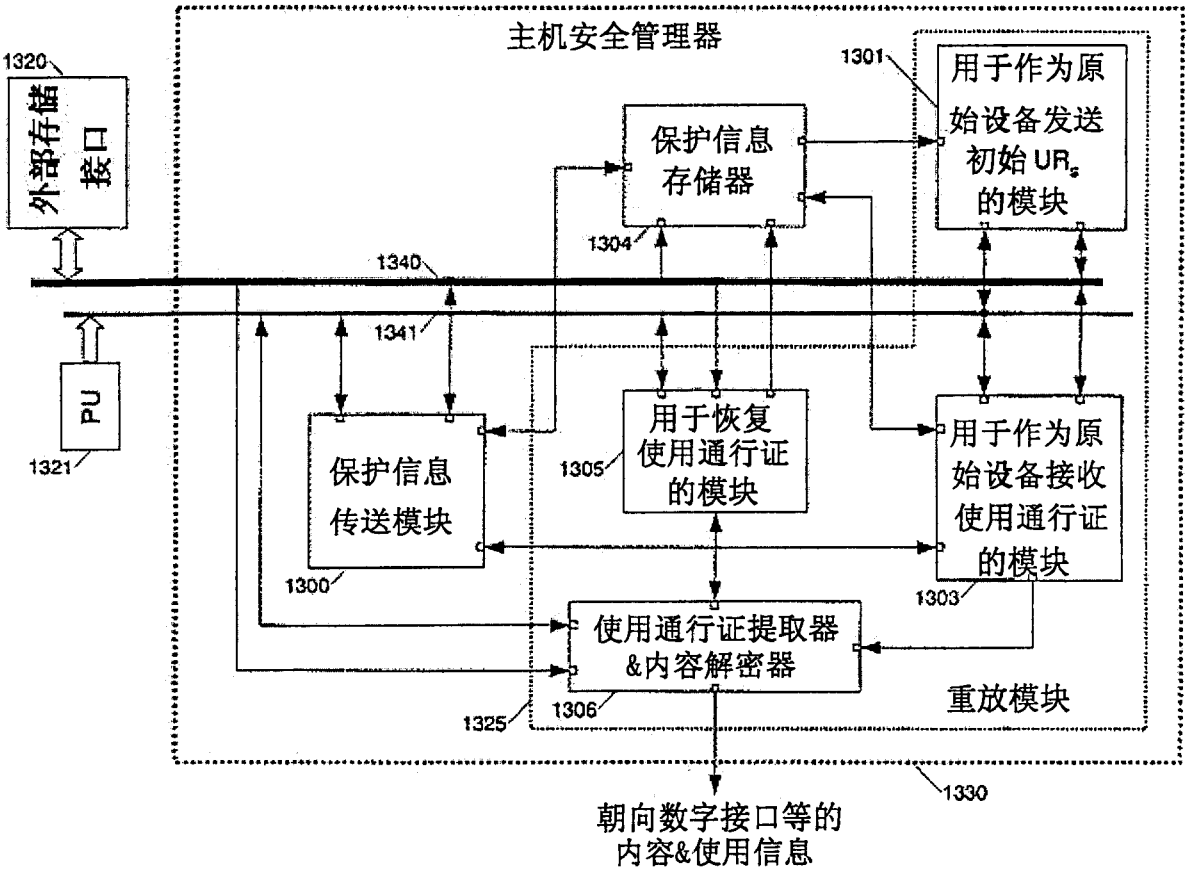

主机安全管理器
1320
外部存储接口
PU
1321
1340
1341
1301
用于作为原始设备发送初始 UR_s 的模块
保护信息存储器
1304
保护信息传送模块
1300
用于恢复使用通行证的模块
1305
用于作为原始设备接收使用通行证的模块
1303
使用通行证提取器&内容解密器
1306
1325
重放模块
1330
朝向数字接口等的内容&使用信息

图13

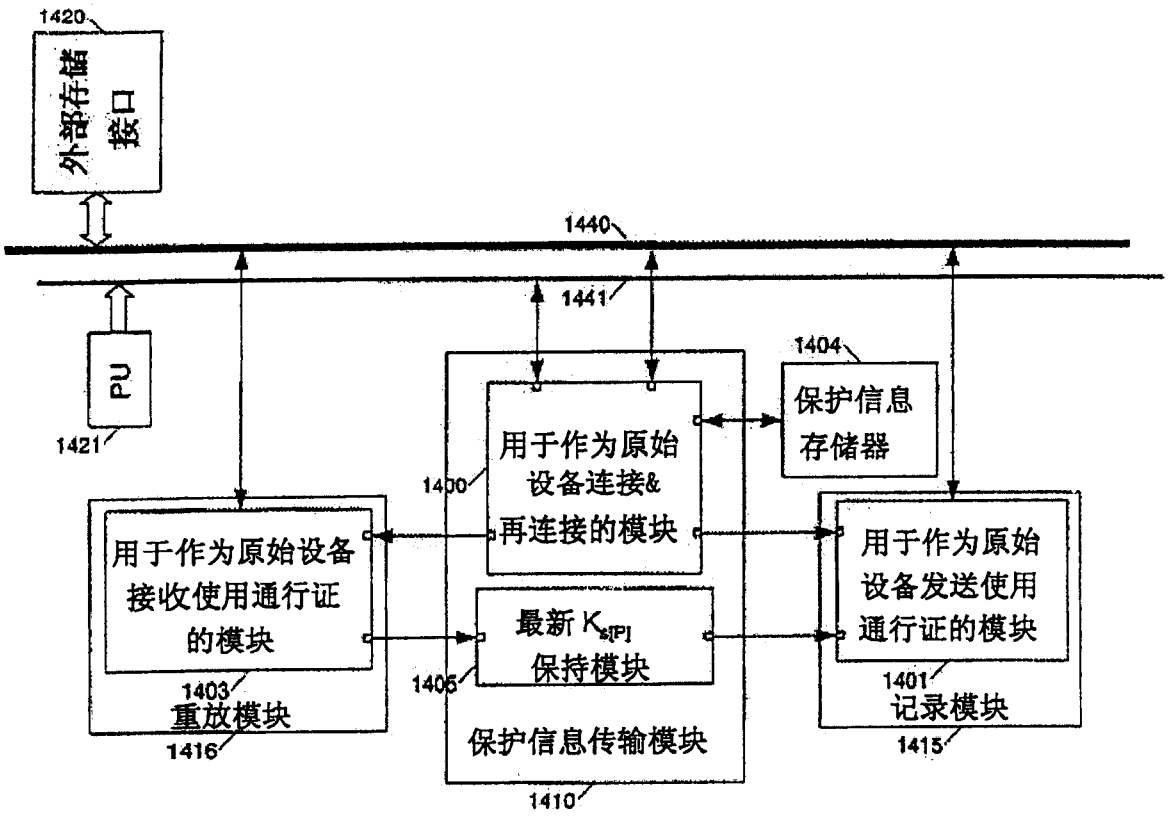

1420
外部存储接口
1440
1441
PU
1421
1404
保护信息存储器
用于作为原始设备连接&再连接的模块
1400
用于作为原始设备接收使用通行证的模块
最新 $K_{s[P]}$ 保持模块
1405
用于作为原始设备发送使用通行证的模块
1403
重放模块
1416
保护信息传输模块
1410
1401
记录模块
1415

图14

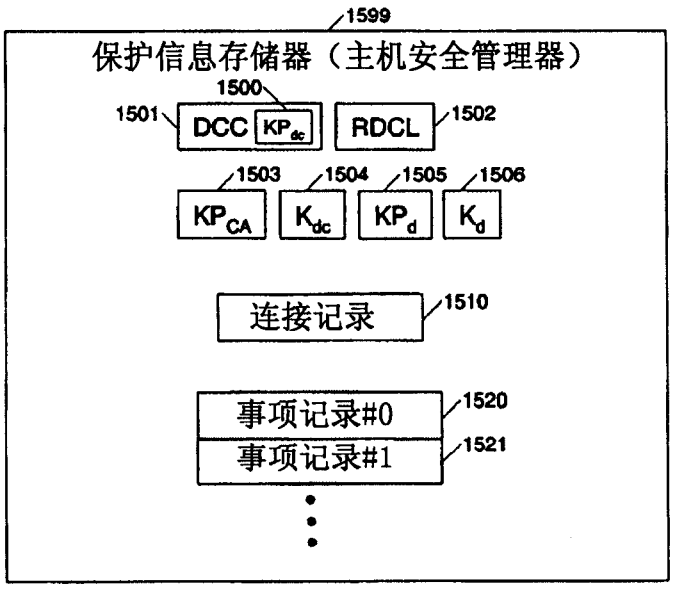

1599
保护信息存储器（主机安全管理器）
1500
1501
DCC KP_{dc}
RDCL
1502
1503
1504
1505
1506
KP_{CA}
K_{dc}
KP_d
K_d
连接记录
1510
事项记录#0
1520
事项记录#1
1521

图15

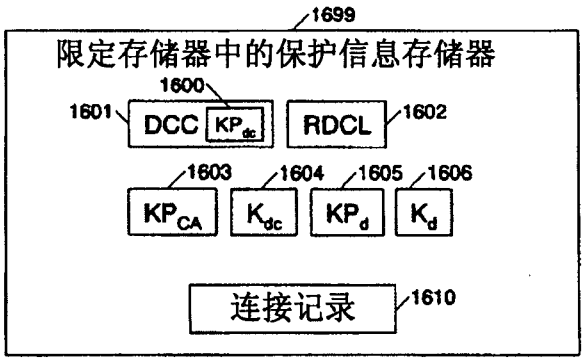


图16

限定访问方式识别顺序

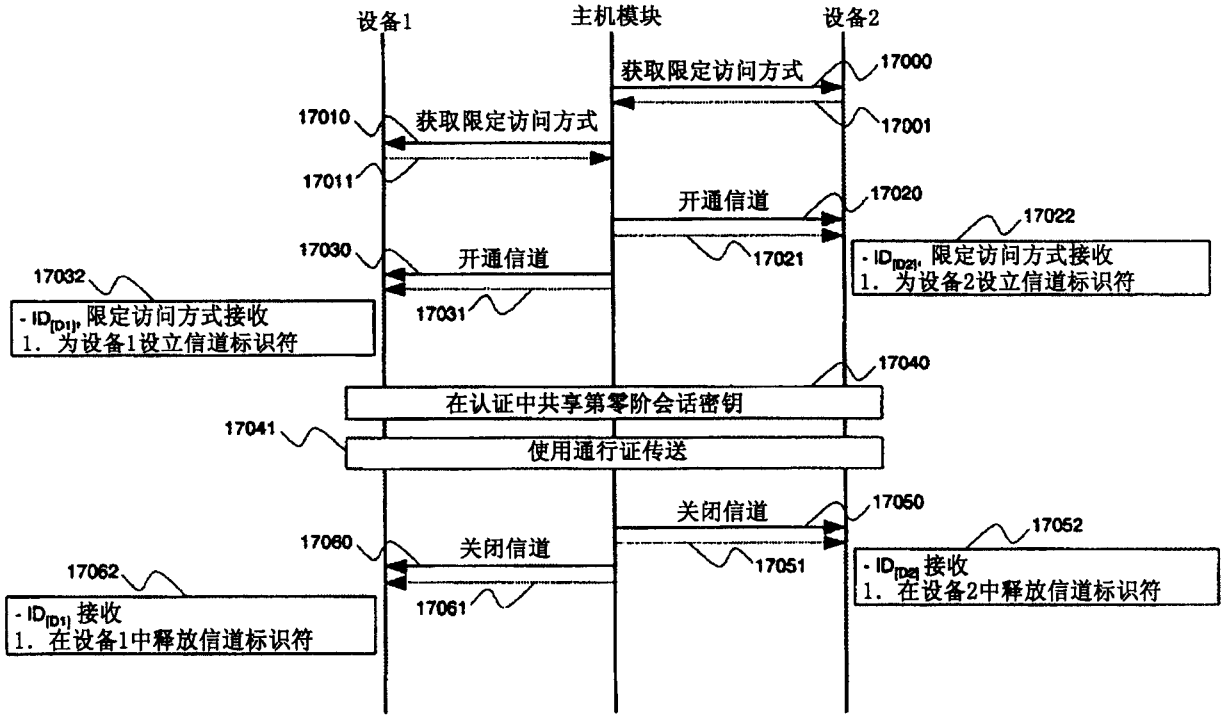


图17

UT方式：连接阶段

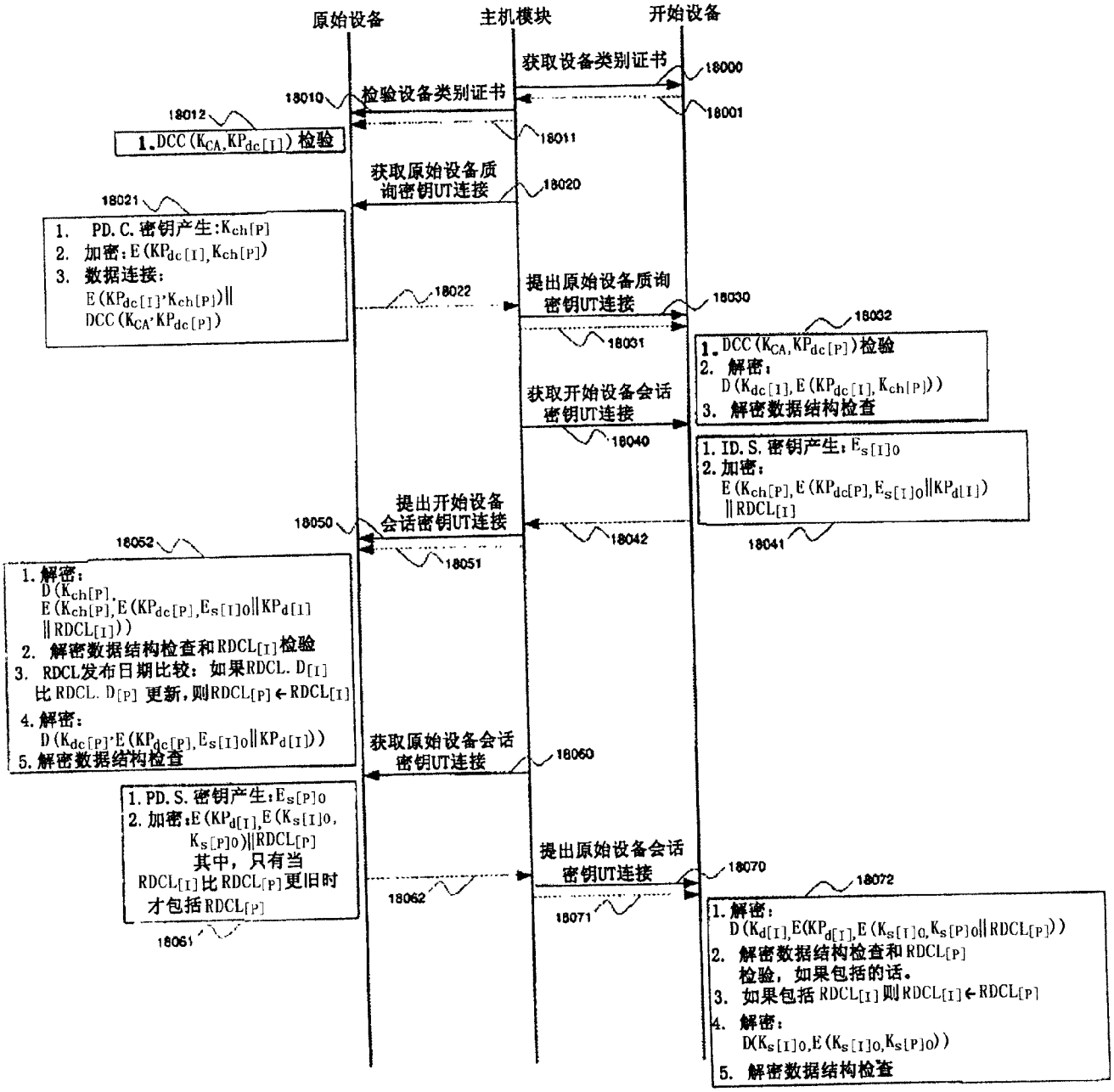


图18

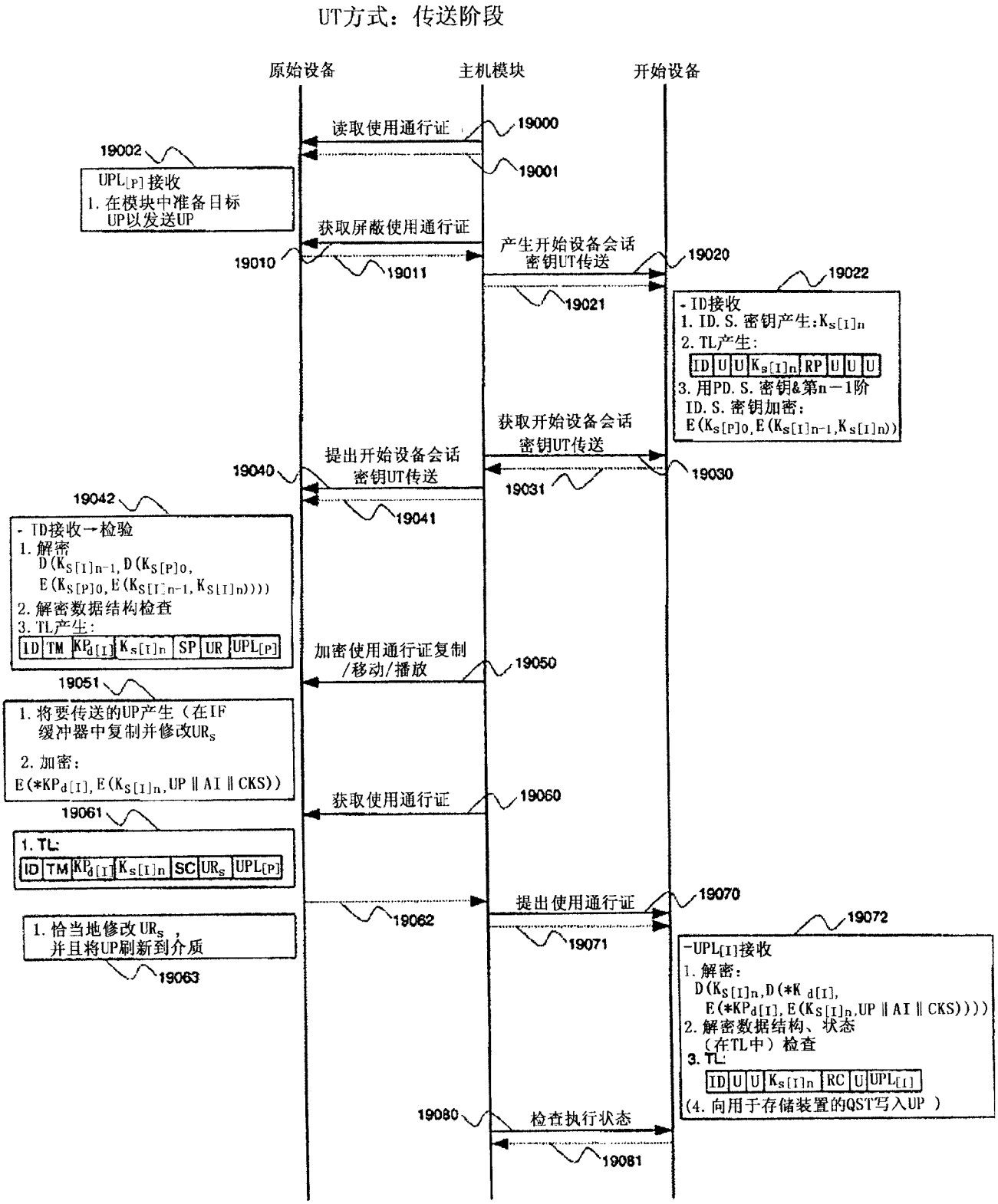

UT方式：传送阶段
原始设备
主机模块
开始设备
读取使用通行证
19000
19001
19002
UPL[P]接收
1. 在模块中准备目标UP以发送UP
获取屏蔽使用通行证
19010
19011
产生开始设备会话密钥UT传送
19020
19021
19022
- ID接收
1. ID. S. 密钥产生:Ks[I]n
2. TL产生:
ID U U Ks[I]n RP U U U
3. 用PD. S. 密钥&第n－1阶ID. S. 密钥加密:
E(Ks[P]0,E(Ks[I]n-1,Ks[I]n))
获取开始设备会话密钥UT传送
19030
19031
提出开始设备会话密钥UT传送
19040
19041
19042
- ID接收→检验
1. 解密
D(Ks[I]n-1,D(Ks[P]0,
E(Ks[P]0,E(Ks[I]n-1,Ks[I]n))))
2. 解密数据结构检查
3. TL产生:
ID TM KPd[I] Ks[I]n SP UR UPL[P]
加密使用通行证复制/移动/播放
19050
19051
1. 将要传送的UP产生（在IF缓冲器中复制并修改URs
2. 加密:
E(*KPd[I],E(Ks[I]n,UP‖AI‖CKS))
获取使用通行证
19060
19061
1. TL:
ID TM KPd[I] Ks[I]n SC URs UPL[P]
19062
提出使用通行证
19070
19071
19072
-UPL[I]接收
1. 解密:
D(Ks[I]n,D(*Kd[I],
E(*KPd[I],E(Ks[I]n,UP‖AI‖CKS))))
2. 解密数据结构、状态（在TL中）检查
3. TL:
ID U U Ks[I]n RC U UPL[I]
(4. 向用于存储装置的QST写入UP)
1. 恰当地修改URs，并且将UP刷新到介质
19063
19080
检查执行状态
19081

图19

UT方式：再连接阶段

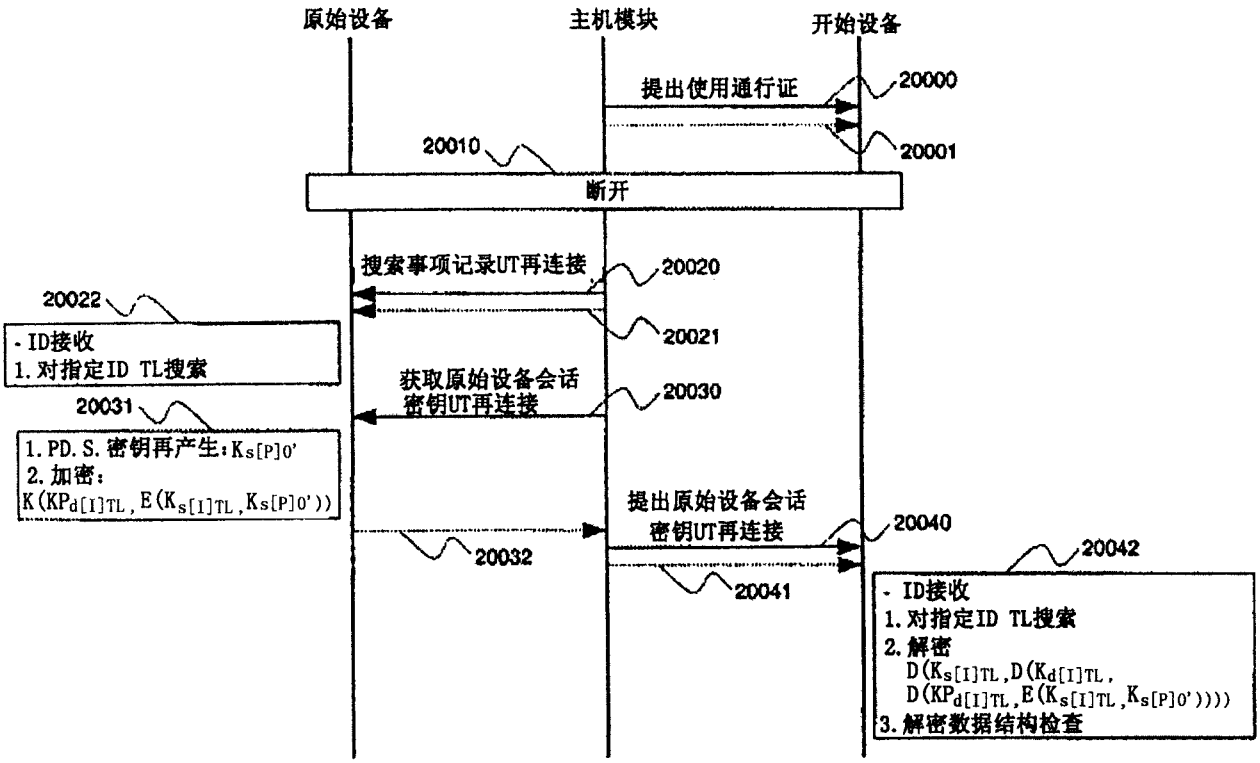


图20

UT方式：恢复阶段

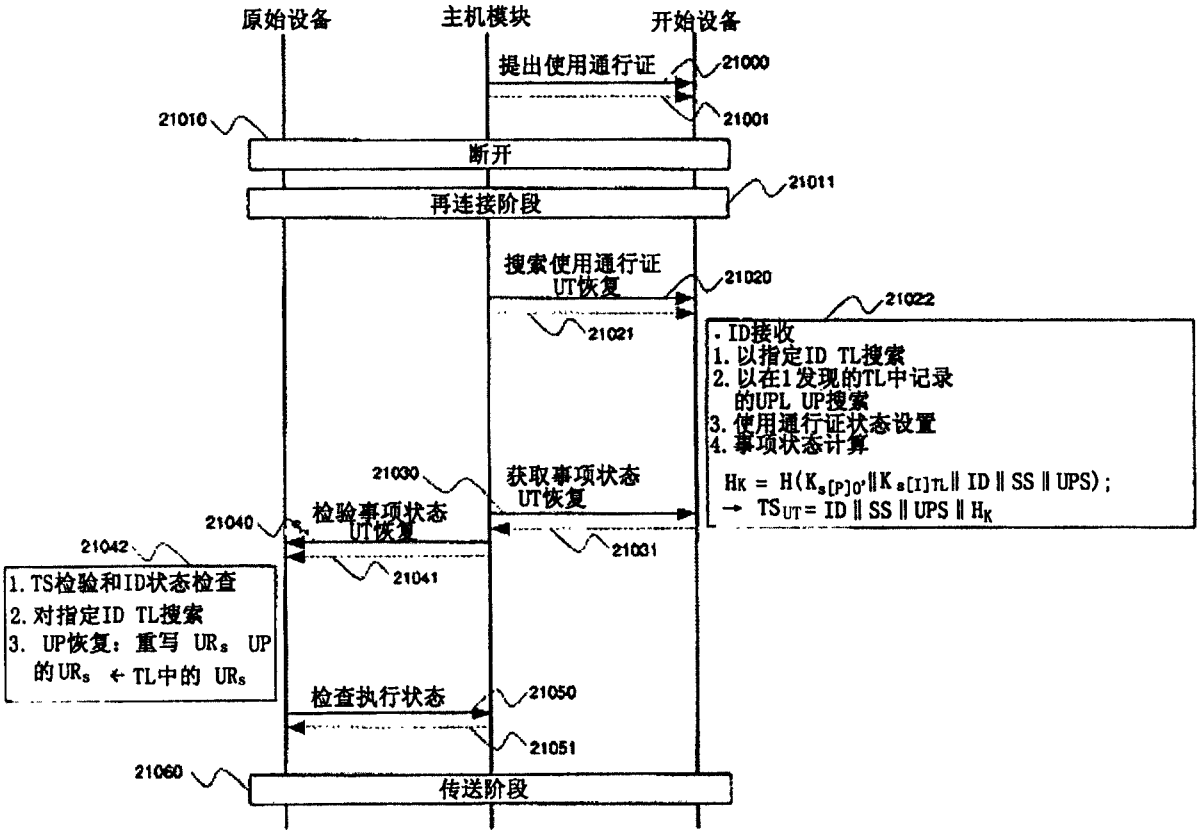


图21

BT方式：连接阶段

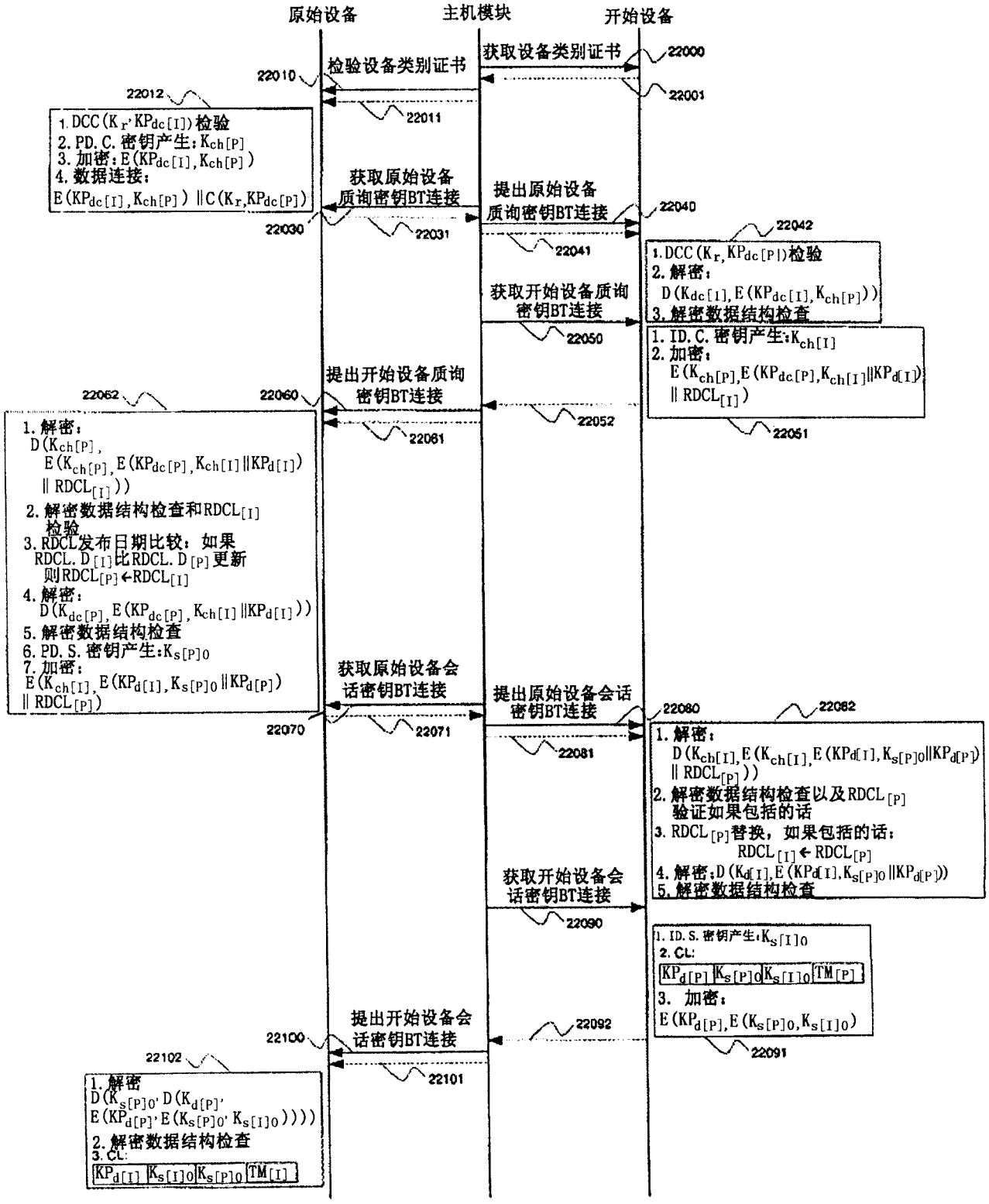


图22

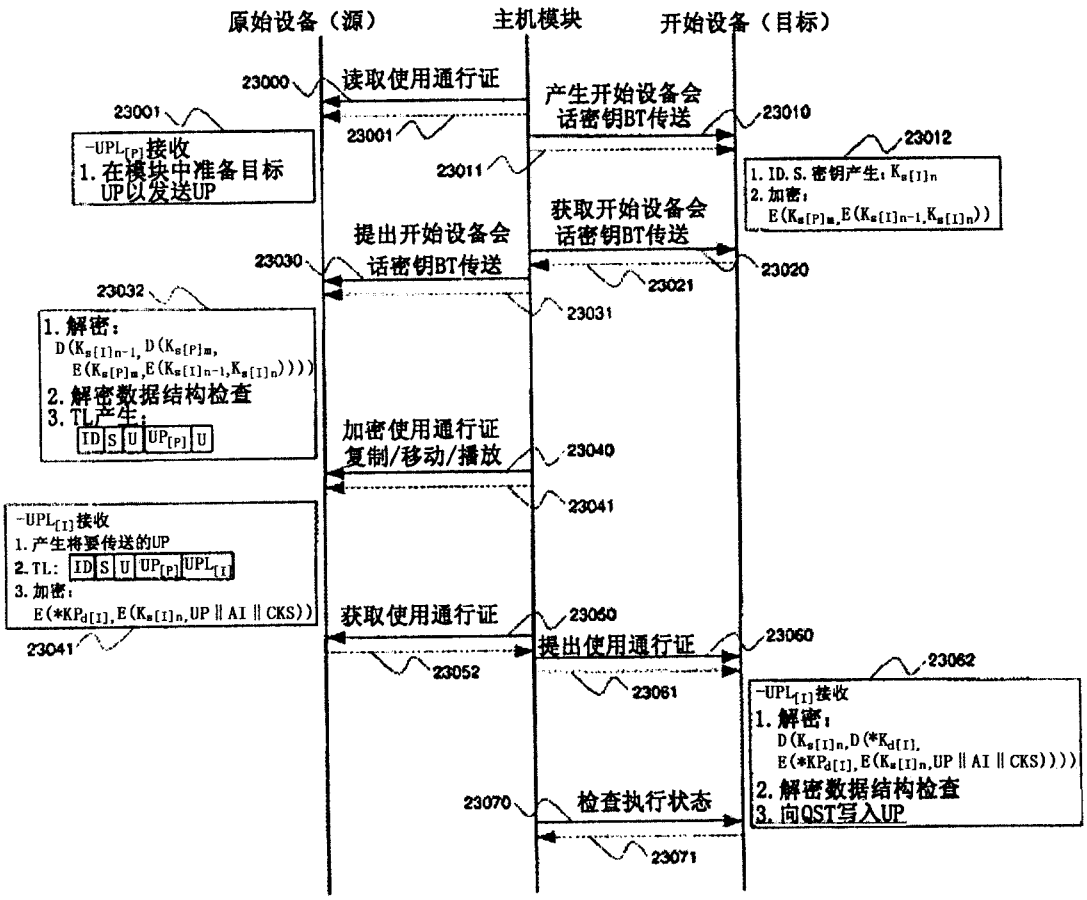

BT方式：传送阶段
原始设备（源）
主机模块
开始设备（目标）
23000
读取使用通行证
23001
23001
-UPL[P]接收
1. 在模块中准备目标UP以发送UP
产生开始设备会话密钥BT传送
23010
23012
23011
1. ID. S. 密钥产生：Ks[I]n
2. 加密：
E(Ks[P]m,E(Ks[I]n-1,Ks[I]n))
获取开始设备会话密钥BT传送
提出开始设备会话密钥BT传送
23030
23020
23021
23032
23031
1. 解密：
D(Ks[I]n-1, D(Ks[P]m,
E(Ks[P]m,E(Ks[I]n-1,Ks[I]n))))
2. 解密数据结构检查
3. TL产生：
ID S U UP[P] U
加密使用通行证复制/移动/播放
23040
23041
-UPL[I]接收
1. 产生将要传送的UP
2. TL: ID S U UP[P] UPL[I]
3. 加密：
E(*KPd[I],E(Ks[I]n,UP‖AI‖CKS))
23041
获取使用通行证
23050
提出使用通行证
23060
23052
23061
23062
-UPL[I]接收
1. 解密：
D(Ks[I]n,D(*Kd[I],
E(*KPd[I],E(Ks[I]n,UP‖AI‖CKS))))
2. 解密数据结构检查
3. 向QST写入UP
23070
检查执行状态
23071

图23

BT方式：传送阶段

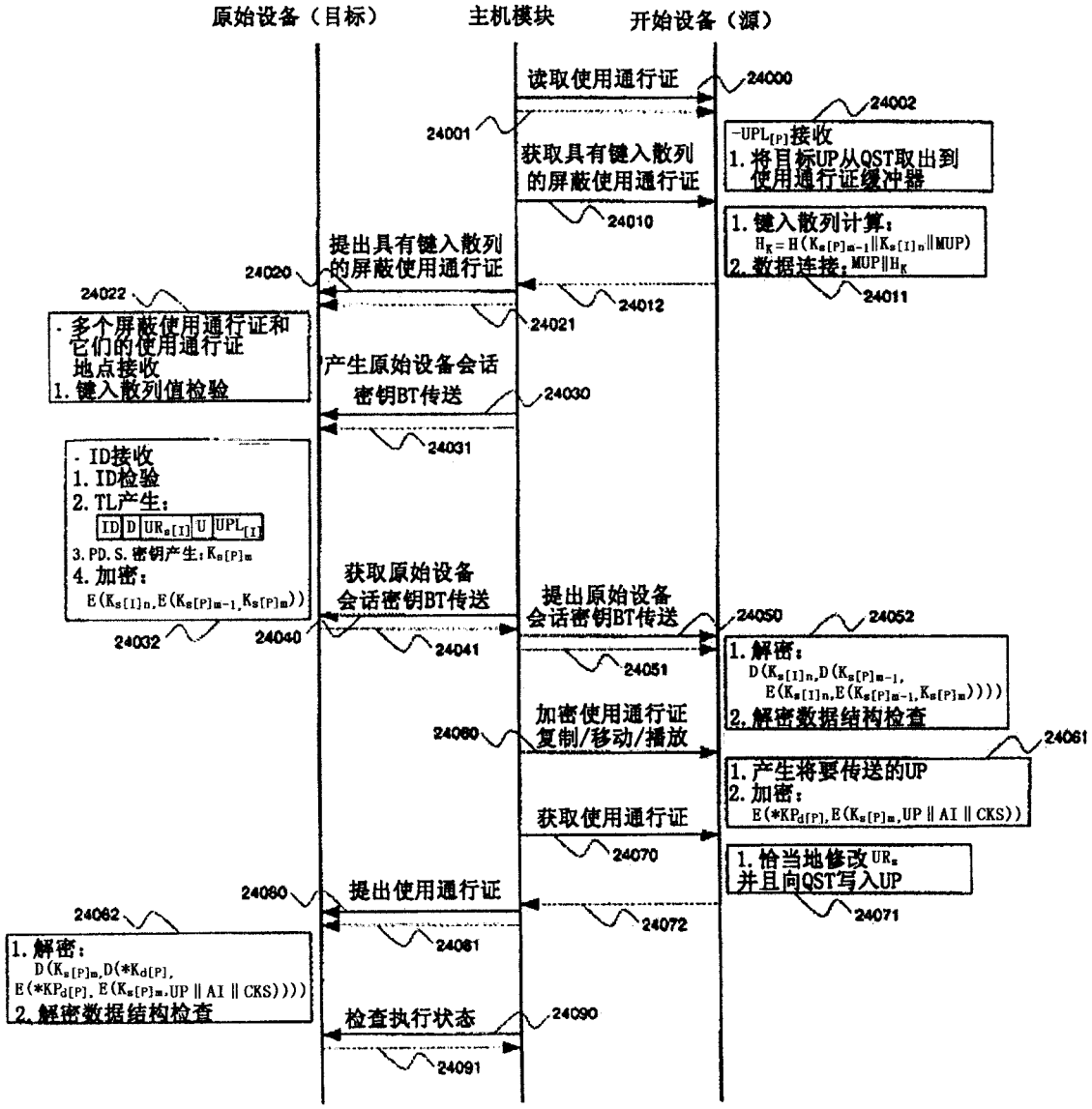


图24

BT方式：再连接阶段

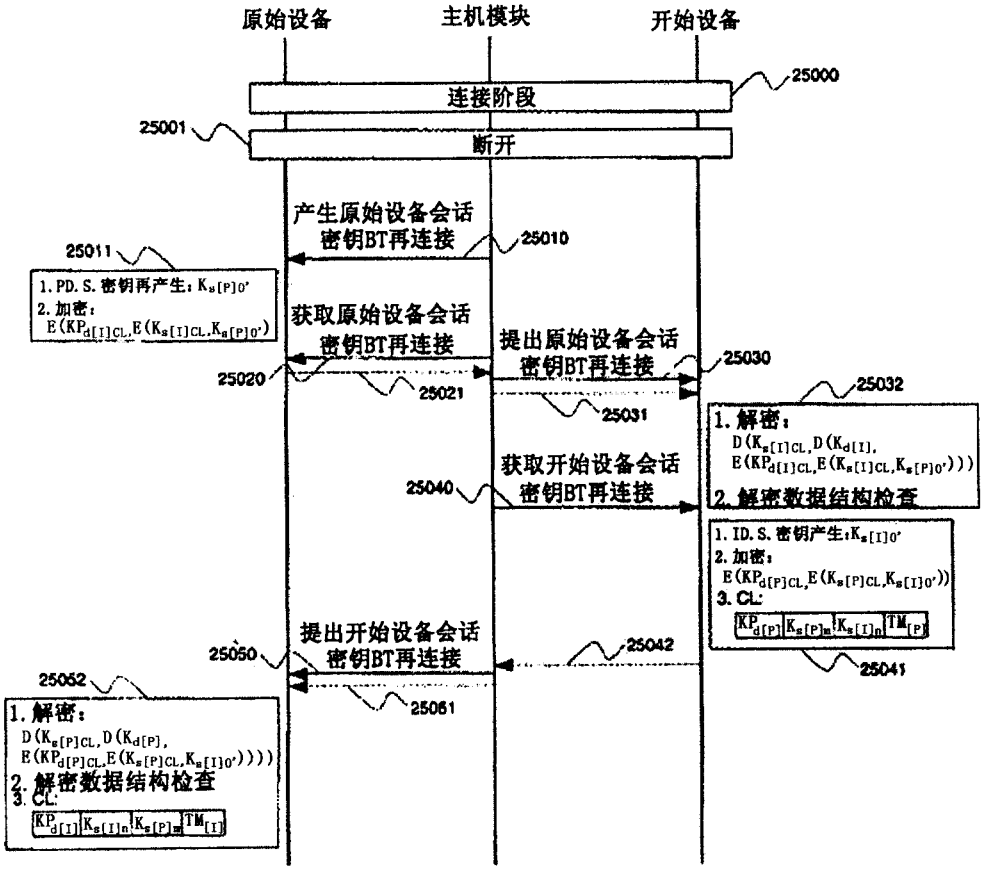


图25

BT方式：恢复阶段

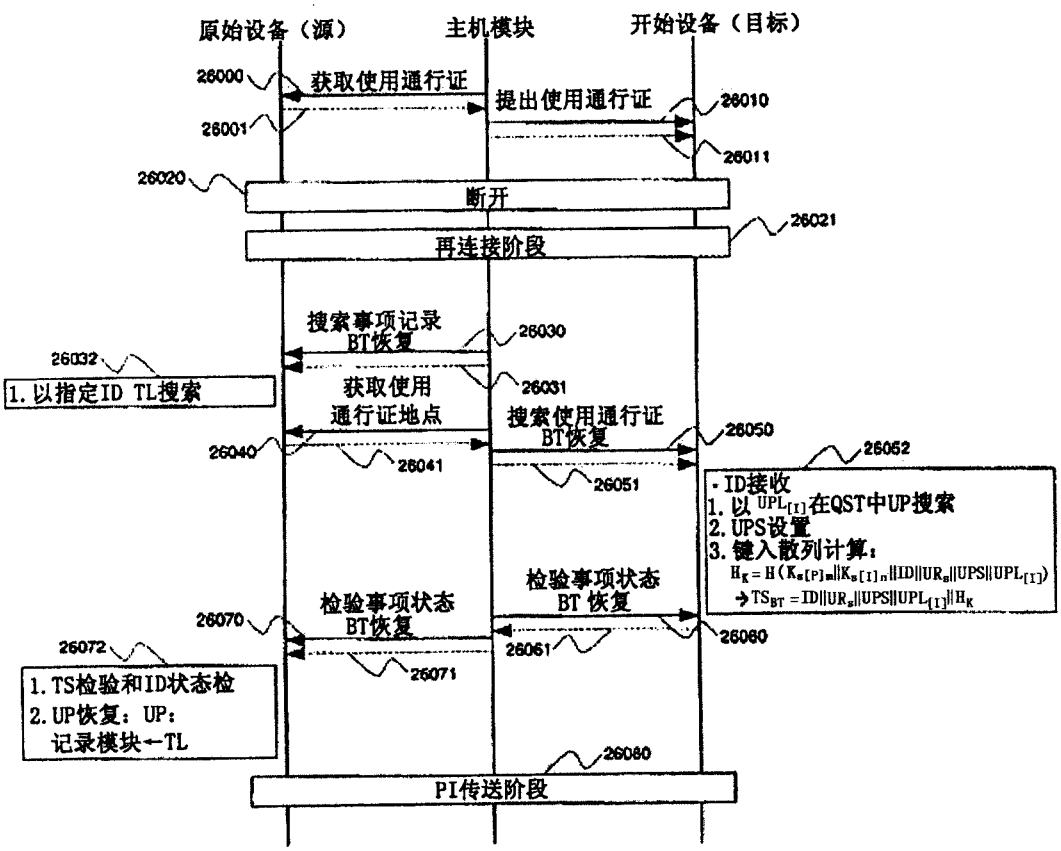


图26

BT方式：恢复阶段

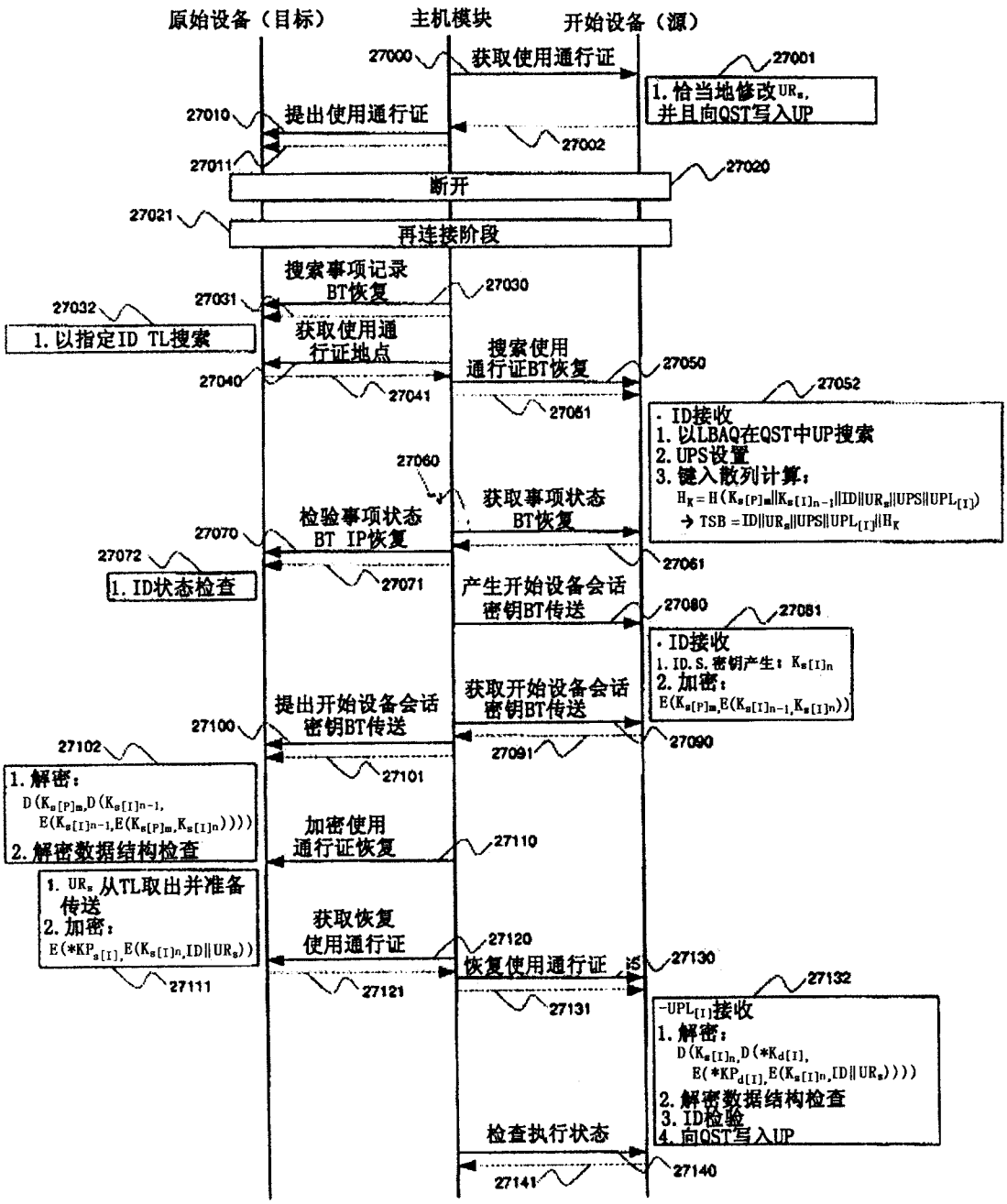


图27

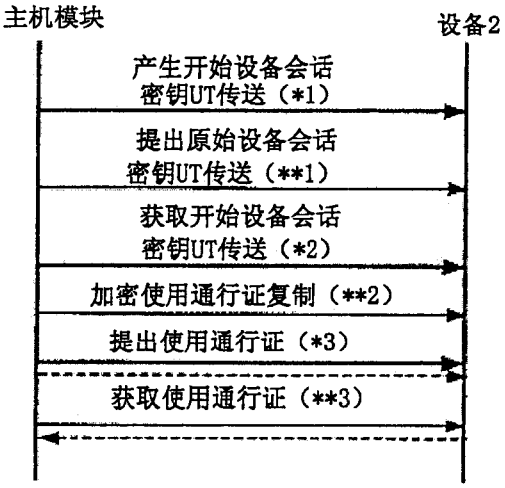

主机模块
设备2
产生开始设备会话
密钥UT传送（*1）
提出原始设备会话
密钥UT传送（**1）
获取开始设备会话
密钥UT传送（*2）
加密使用通行证复制（**2）
提出使用通行证（*3）
获取使用通行证（**3）

图28