[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 12/14
H04N 7/16

[12] 发明专利说明书

[21] ZL 专利号 00117872.5

[45] 授权公告日 2004 年 12 月 1 日

[11] 授权公告号 CN 1178140C

[22] 申请日 2000.4.7 [21] 申请号 00117872.5

[30] 优先权

[32] 1999. 4. 7 [33] JP [31] 099949/1999

[32] 1999. 6.24 [33] JP [31] 178188/1999

[71] 专利权人 索尼公司

地址 日本东京都

[72] 发明人 冈上拓己 木原信之 横田哲平

审查员 杨双翼

[74] 专利代理机构 北京市柳沈律师事务所

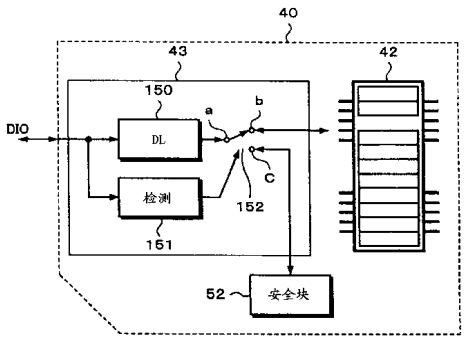
代理人 黄小临

权利要求书 3 页 说明书 24 页 附图 18 页

[54] 发明名称 具增强的兼容性的安全型存储设备、数据处理设备和方法

[57] 摘要

一种存储设备，如存储卡，可分离地连接到诸如数字录像机或音频记录/再现设备的数据处理设备。 存储设备包括非易失性存储器、保护存储在非易失性存储器中的数据的安全性的安全装置、和从数据处理设备接收控制数据的接口。 控制数据或者是对非易失性存储器进行读或写操作的第一控制数据或者是用于所述安全装置的安全操作并且不同于第一控制数据的第二控制数据。 因此，一种安全型存储卡能够与安全型和非安全型数据处理设备兼容。



ISSN1008-4274

权 利 要 求 书

1. 一种可分离地连接到数据处理设备的存储设备，包括:

非易失性存储器;

安全装置，用于保护存储在所述非易失性存储器中的数据的安全性;

接口，用于从数据处理设备接收第一控制数据和第二控制数据，该第二控制数据不同于第一控制数据，所述接口输送所接收的对非易失性存储器进行读或写操作的第一控制数据，并输送所接收的用于所述安全装置的安全操作的第二控制数据;

其中，所述接口包括检测装置和转换装置，该检测装置测定从所述数据处理设备输入的控制数据是所述第一控制数据还是所述第二控制数据，该转换装置依据所述检测装置的检测结果切换所述控制数据，以使所述第一控制数据输送到所述非易失性存储器，而使所述第二控制数据输送到所述安全装置。

2. 如权利要求 1 所述的存储设备，其中，在所述接口接收所述第一或第二控制数据之后，所述接口接收分别由所述第一或第二控制数据定义的数据。

3. 如权利要求 2 所述的存储设备，其中，在所述第一控制数据或第二控制数据之后所接收的数据包括对所述非易失性存储器进行读或写操作的第一指令和用于安全操作的且不同于所述第一指令的第二指令。

4. 如权利要求 3 所述的存储设备，其中，所述接口输送对所述非易失性存储器进行读或写操作的所述第一指令，并输送对所述安全装置的安全操作的第二指令。

5. 如权利要求 1 所述的存储设备，其中，所述接口将所述第一控制数据输出到连接在所述接口和所述非易失性存储器之间的页面缓冲器、写寄存器和读寄存器中的至少一个中。

6. 如权利要求 1 所述的存储设备，其中，所述存储设备可分离地连接到非安全型数据处理设备，该非安全型数据处理设备可操作该存储设备，并且该非安全型数据处理设备发送所述第一控制数据而不发送所述第二控制数据，所述存储设备还可分离地连接到安全型数据处理设备，该安全型数据处理设备可操作该存储设备，并且该安全型数据处理设备发送所述第

一和第二控制数据。

7. 如权利要求 6 所述的存储设备，其中，非安全型和安全型数据处理设备分别从由下述装置组成的组中选择：音频记录器/播放器和图像记录/再现设备。

8. 如权利要求 1 所述的存储设备，其中，所述安全装置被构造成：通过共享对话密钥与所述数据处理设备的安全装置相联系地保护存储在非易失性存储器中的数据的安全性。

9. 一种数据处理设备，该数据处理设备用于将数据记录到与其可分离地连接的存储设备中，该存储设备具有非易失性存储器和安全装置，所述数据处理设备包括：

与所述存储设备进行通信的接口，和

安全装置，该安全装置协同所述存储设备的安全装置保护存储在非易失性存储器中的数据的安全性。

其中，所述数据处理设备通过所述接口发送对非易失性存储器进行读或写操作的第一控制数据、和不同于所述第一控制数据用于安全操作的第二控制数据。

10. 如权利要求 9 所述的数据处理设备，其中，在发送所述第一或第二控制数据之后，所述数据处理设备发送分别由第一或第二控制数据所定义的数据。

11. 如权利要求 10 所述的数据处理设备，其中，在所述第一控制数据或第二控制数据之后发送的数据包括对所述非易失性存储器进行读或写操作的第一指令、和用于安全操作且不同于所述第一指令的第二指令。

12. 一种数据处理系统，其具有数据处理设备和可分离地连接到所述数据处理设备的存储设备，所述存储设备具有非易失性存储器和安全装置，

其中，所述数据处理设备包括安全装置，该安全装置协同所述存储设备的安全装置保护存储在非易失性存储器中数据的安全性，

所述数据处理设备还包括在所述数据处理设备和所述存储设备之中的接口装置，其中通过所述接口装置从所述数据处理设备向所述存储设备发送对非易失性存储器进行读或写操作的第一控制数据、和不同于所述第一控制数据用于安全操作的第二控制数据；

其中，所述接口包括检测装置和转换装置，该检测装置测定从所述数

据处理设备输入的控制数据是所述第一控制数据还是所述第二控制数据，该转换装置依据所述检测装置的检测结果切换所述控制数据，以使所述第一控制数据输送到所述非易失性存储器，而使所述第二控制数据输送到所述安全装置。

13. 一种用于数据处理系统中的数据处理方法，该数据处理系统具有数据处理设备和可分离地连接到所述数据处理设备的存储设备，所述存储设备包括非易失性存储器和安全装置，该安全装置用于保护存储在所述非易失性存储器中的数据的安全性，所述方法包括下列步骤：

从所述数据处理设备有选择性地向所述存储设备发送第一控制数据或第二控制数据，该第一控制数据用于对非易失性存储器进行读或写操作，该第二控制数据不同于所述第一控制数据，它是用于安全操作的；以及

所述存储设备接收所述发送的控制数据，确定它是第一控制数据还是第二控制数据，并将所接收的第一控制数据输送到所述非易失性存储器，而将所述第二控制数据输送到所述安全装置。

14. 一种用于存储设备中的方法，该存储设备可分离地连接到数据处理设备，所述存储设备包括非易失性存储器和用于保护存储在所述非易失性存储器中的数据的安全性的安全设备，所述方法包括下列步骤：

所述存储设备接收由数据处理设备发送的控制数据，所述控制数据或者是用于对非易失性存储器进行读或写操作的第一控制数据、或者是不同于所述第一控制数据并用于安全操作的第二控制数据；和

确定所接收的控制数据是第一控制数据还是第二控制数据，并将所接收的第一控制数据输送到所述非易失性存储器，而将所述第二控制数据输送到所述安全装置。

说　明　书

具增强的兼容性的
安全型存储设备、数据处理设备和方法

技术领域

本发明一般涉及数据安全性(security)，更具体地说，涉及一种可分离地连接到数据处理设备的存储设备，比如存储卡，该存储设备包括数据安全装置。

背景技术

在常规的非易失性存储器比如 EEPROM(电可擦除可编程序只读存储器)中，应用两个晶体管来存储一个信息位。因此，每个位的存储面积较大，这就限制了对存储器的集成能力的提高。在另一方面，在近年来开发的闪速存储器中消除了这种问题，在该闪速存储器中依据“全位同时擦除”方法应用单个晶体管来存储一个位。预计在不远的将来闪速存储器将取代常规的记录媒体比如大量应用的磁盘和光盘。

可分离地连接到存储卡读/记录装置的基于闪速存储器的存储卡或“memory sticks™”已为大家所熟悉。由于出现了这种类型的存储卡，人们应用这种存储卡取代常规的盘形媒体比如 CD(光盘)或小型盘开发了数字音频记录/再现设备。

应用存储卡作为记录媒体的音频记录器一般应用一种数据压缩方法，该方法能够以相对较高的质量恢复数据进行记录/再现。可以应用加密技术来保护以这种录音机记录和复制的曲目的版权。作为一个实例，应用加密技术设计录音机使其能够确定存储卡是否为非法，如果确定为非法则禁止该录音机使用。换句话说，只有合法的录音机和合法的存储卡相结合才能对经加密的数据进行解密。除了版权保护外，还可以应用加密技术来保护存储在存储卡中的其它信息的安全。

常规的存储卡并不具有加密功能。因此，当将秘密数据记录到存储卡上时，在“设备”侧(即在该存储卡所插入的装置(设备)中)对数据进行加密，该设备编排该数据进行记录。然后将经加密的数据传送到存储卡进行存储。

如果将解密密钥也存储在该存储卡中，就会危及到存储在存储卡中的数据的安全性。另一方面，当将解密密钥存储在特定的设备中时，不能通过除了该特定的设备以外的其它设备来解密最初由该设备加密并记录在存储卡中的数据。因此，不能保证存储卡的兼容性。为解决这个问题，人们已经提出了一种系统，在该系统中设备和存储卡各自都具有加密功能，由此使该设备和该存储卡能够相互验证。在这种情况下可以认为存储卡为“智能卡”，其具有能够对数据进行加密的处理电路。应用这种方法能够确保数据的安全性和兼容性。

具有上述验证和加密功能的安全设备可以依据数据加密标准(DES)进行加密。该 DES 是一种块加密系统，在该系统中文本是以块分段的，并对每个块段进行加密。应用 DES 时，应用 64 位(实际上密钥为 56 位，其它 8 位校验位)的密钥对 64 位的输入数据进行加密，然后输出经加密的 64 位数据。DES 具有四种应用模式，一种为密码块链接(CBC)模式。该 CBC 模式是一种反馈式模式，在该模式中对 64 位文本和在先加密的数据(64 位)进行异或，将所得到的结果输入到 DES 单元中。在开始时，由于没有加密数据，因此应用初始化矢量。此外，当在该设备和该存储卡之间进行数据交换时，产生随机数据并将该随机数据加入到该数据中。

在许多应用场合需要将不具有版权的数据记录到存储卡并从其中再现。这些应用的例子包括会话语音的记录(在存储该数据之前一般要以较高的压缩比进行压缩)、来自电子静止照相机或摄影机的图像数据等。在这些情况下不需要保护数据版权的装置。通常，具有加密功能的安全型存储卡比非安全型存储卡(即，常规的存储卡)更昂贵。因此，安全型存储卡(及相关设备)应用在它所需要的应用系统中，而非安全型存储卡和设备可以应用在其它应用系统中以降低成本。已有技术中的安全型设备只可以应用安全型存储卡，并且非安全型设备只可能应用非安全型存储卡。

发明内容

本发明考虑到，基于兼容性，希望应用安全型存储卡的应用情况下也可以使用非安全型设备(例如常规的设备)。在这些应用情况下，例如记录来自便携式录像机的图像数据，不应用存储卡的加密功能。

因此，本发明的一个目的为提供一种安全型存储设备，其能够应用安

全型和非安全型数据处理单元(设备)。

本发明的另一个目的为提供一种能够与存储卡兼容的数据处理设备，其给存储卡传输不同类型的控制数据以执行不同的功能。

在本发明的一方面，提供一种能够可分离地连接到数据处理设备(比如数字录象机或音频记录/再现设备)的存储设备。该存储设备包括非易失性存储器、保护存储在非易失性存储器中的数据的安全性的安全装置、和从数据处理设备接收控制数据的接口。其中，所述接口包括检测装置和转换装置，该检测装置测定从所述数据处理设备输入的控制数据是所述第一控制数据还是所述第二控制数据，该转换装置依据所述检测装置的检测结果切换所述控制数据，以使所述第一控制数据输送到所述非易失性存储器，而使所述第二控制数据输送到所述安全装置。控制数据是用于对非易失性存储器进行读或写操作的第一控制数据，或者控制数据是用于安全装置的安全操作的第二控制数据(与第一控制数据不同)。因此，不仅安全型而且非安全型数据处理单元(设备)都能够应用该存储设备。非安全型设备仅发送第一控制数据，该第一控制数据用于向存储设备存储数据和/或从存储设备检索数据(其为非加密数据)。通过给存储设备发送第一和第二控制数据，安全型设备保护存储在非易失性存储器中的数据的安全性。因此，安全型数据处理设备不仅能够应用安全型存储器，还能够应用非安全型存储卡。因此，提高了安全型存储设备的兼容性。

在本发明的另一方面，提供一种数据处理设备，以将数据记录到可分离地连接的存储设备中，这里存储设备具有非易失性存储器和安全单元。数据处理设备包括与存储设备进行通信的接口、和协同存储设备的安全单元保护存储在非易失性存储器中的数据的安全性的安全块。数据处理设备通过接口发送第一控制数据和用于安全操作的第二控制数据，该第一控制数据用于对非易失性存储器进行读或写操作，且该第二控制数据不同于第一控制数据。

在本发明的另一方面，提供一种数据处理系统，其具有数据处理设备和可分离地连接到所述数据处理设备的存储设备，所述存储设备具有非易失性存储器和安全装置，其中，所述数据处理设备包括安全装置，该安全装置协同所述存储设备的安全装置保护存储在非易失性存储器中数据的安全性，所述数据处理设备还包括在所述数据处理设备和所述存储设备之中

的接口装置，其中通过所述接口装置从所述数据处理设备向所述存储设备发送对非易失性存储器进行读或写操作的第一控制数据、和不同于所述第一控制数据用于安全操作的第二控制数据；其中，所述接口包括检测装置和转换装置，该检测装置测定从所述数据处理设备输入的控制数据是所述第一控制数据还是所述第二控制数据，该转换装置依据所述检测装置的检测结果切换所述控制数据，以使所述第一控制数据输送到所述非易失性存储器，而使所述第二控制数据输送到所述安全装置。

附图说明

通过下文结合附图的详细描述，本发明的上述目的以及其它目的、特征和优点将会更清楚。在附图中：

附图 1 描述了依据本发明的一个实施例的记录器/播放器(录/放机)和存储卡的整体结构；

附图 2 描述了依据本发明的一个实施例的安全型存储卡的内部结构；

附图 3 描述了依据本发明的一个实施例的非安全型存储卡的内部结构；

附图 4 描述了依据本发明的一个实施例闪速存储器的文件系统处理分级结构图；

附图 5 所示为闪速存储器的物理数据结构的格式；

附图 6 描述了闪速存储器的引导块的结构；

附图 7 描述了闪速存储器的引导块的引导信息和属性信息的结构；

附图 8A 和 8B 所示为在内容和密钥之间的关系；

附图 9 所示为用于解释在记录操作中加密过程的示意图；

附图 10 所示为用于解释验证过程的示意图；

附图 11 所示为用于解释在记录操作中加密过程的示意图；

附图 12 所示为用于解释在再现操作中的加密过程的示意图；

附图 13 所示为用于解释在再现操作中的加密过程的示意图；

附图 14 所示为用于解释设置在记录器和存储卡之间的接口的操作的示意图；

附图 15 所示为用于解释设置在记录器和存储卡之间的接口的操作的示意图；

附图 16 所示为用于本发明的实施例的协议指令的实例表；

附图 17-18 所示为用于本发明的实施例中的指令的表；和

附图 19 所示为依据本发明的存储设备的示意性方块图。

具体实施方式

附图 1 所示为依据本发明的一个优选实施例的数字音频记录器/播放器(数字录/放机)1 的结构的方块图。数字音频记录器/播放器 1 应用可分离的存储卡(或 memory sticks™)40 来记录和再现数字音频信号。记录器/播放器 1 可以是具有如下设备的音频系统的一部分：放大单元(未示)、扬声器(未示)、CD 播放器(未示)、MD 记录器(未示)、调谐器(未示)等等。然而，应注意的是，本发明还可以应用在其它音频设备中。例如，记录器/播放器 1 可以是便携式设备。本发明还可以应用在机顶盒中，该机顶盒记录经过卫星数据通信、数字广播或因特网等流通的数字音频数据。此外，本发明还可以应用在记录/再现除音频数据以外的运动图像数据和静止图像数据的系统中。依据本发明实施例的系统还可以记录和再现除了数字音频信号以外的其它信息比如图像和文本。

记录器/播放器 1(也可以将其看作数据处理设备)具有中央处理器(CPU)2、安全块 3、操作按键 4 和显示装置 5。安全块 3、操作按键 4 和显示装置 5 通过总线 16 连接到 CPU 2。安全块 3 包括数据加密标准(DES)加密电路。通过总线 16 将数据(比如记录指令、再现指令或与用户对按键 4 的操作相对应的其它指令)输入到 CPU 2 中。各种信息、记录器/播放器 1 的操作状态等都显示在显示装置 5 上。音频接口 6 设置在外部输入/输出端(在下文将对其作进一步的详细描述)和内部音频编码器/解码器 7 之间。

如下文将要描述的，存储卡 40 是一种 IC 芯片，其具有闪速存储器(非易失性存储器)42、控制块 41、安全块 52(安全块 52 可能包括 DES 加密电路)、通信接口、寄存器等。存储卡 40 可连接到记录器/播放器 1 上，并且也可以与其分离开。依据一个实施例，记录器/播放器 1 还可以与并不具有加密功能(即，安全块 52)的存储卡兼容。

音频编码器/解码器 7 依据写到存储卡 40 中的高效编码方法对数字音频数据进行编码。此外，编码器/解码器 7 还对从存储卡 40 中读出的已经编码的数据进行解码。可以应用高效 ATRAC 3 格式编码方法，该方法是一种用于 MD 的自适应变换声音编码(ATRAC)格式的改进。

在 ATRAC 3 格式中，对以 44.1 千赫兹(kHz)采样、以 16 位进行量化的音频数据以高效率编码。处理音频数据的最小数据单元是一声音单元(SU)。1 个 SU 包含 1024 个采样数据，因此包含(1024 × 16 位 × 2 声道)位的数据，该数据被压缩成几百个字节的数据。1 个 SU 的持续时间大约为 23 毫秒。在应用这种高效的编码方法的情况下，被压缩的数据的大小大约比原始数据小 10 倍。与应用在 MD 中的 ATRAC 1 格式相比，依据 ATRAC 3 格式压缩和解压的音频信号的音频质量更好。

示例性地，模拟输入端 8 将 MD、调谐器或磁带的再现输出信号输送给模拟-数字(A/D)转换器 9。A/D 转换器 9 将来自模拟输入端 8 的信号转换为数字音频信号(采样频率为 44.1kHz，量化位数 = 16)，并将经转换过的音频信号输送到音频接口 6 中。数字输入端 10 将 MD、CD、数字广播信号或网络流通的音频数据的数字输出信号输送给音频接口 6。例如通过光缆传输数字输入信号。音频接口 6 从 A/D 转换器 9 和数字输入端 10 中选择一种输入的数字音频信号，并将所选择的输入的数字音频信号输送给音频编码器/解码器 7。

音频编码器/解码器 7 对输入的数字音频信号进行编码，并将编码后的数据输入到安全块 3 中。安全块 3 对从编码器/解码器 7 中接收到的经编码的数据进行加密，以便保护所述数据(在本实例中，数字音频信号)的内容的版权。记录器/播放器 1 的安全块 3 可以具有许多的主密钥和设备专用存储密钥。此外，安全块 3 可能具有随机数产生电路(未示)。当将具有安全块 52 的存储卡 40 与记录器/播放器 1 相连接时，记录器/播放器 1 的安全块 3 判定存储卡 40 是否为合法的(验证存储卡 40)。在记录器/播放器 1 的安全块 3 确认存储卡 40 合格后，记录器/播放器 1 的安全块 3 和存储卡 40 的安全块 52 才共享对话密钥。

将从安全块 3 输出的经加密的音频数据输送到 CPU 2。CPU 2 通过双向串行接口 11 与存储卡 40 进行通信。在本实施例中，存储卡 40 加到记录

器/播放器 1 的连接/分离机构(未示)。CPU 2 将经加密的数据写入存储卡 40 的闪速存储器 42 中。在 CPU 2 和存储卡 40 之间串行传输经加密的数据。

CPU 2 通过存储器接口 11 从存储卡 40 中读取加密的数据，并将这种数据输送到安全块 3 中。安全块 3 对经加密的音频数据进行解密。将经解码的音频数据输送到音频编码器/解码器 7，该编码器/解码器 7 对经解密的音频数据进行解码。通过音频接口 6 将编码器/解码器 7 的输出信号输送到 D/A 转换器 12。D/A 转换器 12 将数字音频数据转换为模拟音频信号，并通过输出端 13 传输该模拟音频信号。通过接口 16 也可以分别将接收自编码器/解码器 7 的音频数据和接收自安全块 3 的解密数据经过输出端 14 和 15 作为数字输出信号输出。

附图 2 所示为存储卡 40 的内部结构方框图。存储卡 40 是一种包括控制块 41、安全块 52 和闪速存储器 42 的单片集成电路(IC)。如附图 2 所示，设置在记录器/播放器 1 的 CPU 2 和存储卡 40 之间的双向串行接口 11 包括 10 根引线，该 10 根线分别包括：一根用于将时钟信号同数据一道传输的时钟线 SCK、一根传输状态信号的状态线 SBS、一根传输数据的数据线 DIO、一根中断线 INT、两根 GND 线、两根 VCC 线和两根预留线。

在这 10 根线中主要的四根线为时钟线 SCK、状态线 SBS、数据线 DIO 和中断线 INT。时钟线 SCK 用于发送时钟信号使数据传输同步。状态线 SBS 用于发送表示存储卡 40 的状态的状态信号。数据线 DIO 用于输入和输出指令和经加密的音频数据。中断线 INT 用于将中断请求信号从存储卡 40 发送到记录器/播放器 1 的 CPU 2。当将存储卡 40 连接到记录器/播放器 1 时，产生中断信号。在另一个实施例中，经过数据线 DIO 发送中断信号，在这种情况下中断线 INT 接地不使用。

串行/并行和并行/串行接口块(S/P 和 P/S IF 块)43 是一种连接到接口 11 的控制块 41 的接口。S/P 和 P/S IF 块 43 将接收自记录器/播放器 1 的串行数据转换为并行数据。它还可以将控制块 41 的并行数据转换为串行数据，并将串行数据输送到记录器/播放器 1。此外，S/P 和 P/S IF 块 43 将通过数据线 DIO 接收的指令和数据分成用于存取闪速存储器 42 的指令和数据和用于执行加密处理的指令和数据。

换句话说，在发送指令后，应用数据线 DIO 发送数据。S/P 和 P/S IF 块 43 通过所接收的指令代码来确定所接收的指令和数据是用于存取闪速存储

器 42 还是用于进行加密处理的。与所确定结果相对应，将用于存取闪速存储器 42 的指令存储在指令寄存器 44 中，而将数据存储在页面缓冲器 45 和写寄存器 46 中。与写寄存器 46 相关联，设置纠错码编码电路 47 。纠错码编码电路 47 产生用于临时存储在页面缓冲器 45 中的数据的纠错码的冗余码。

将指令寄存器 44 、页面(page)缓冲器 45 、写寄存器 46 、纠错码编码电路 47 的输出数据输送到闪速存储器接口和序列化器(存储器 IF 和序列化器)51 中。存储器 IF 和序列化器 51 是连接到闪速存储器 42 的接口，并且其控制在闪速存储器 42 和控制块 41 之间交换的数据，例如通过存储器 IF 和序列化器 51 将数据写入闪速存储器 42 中。

通过存储器 IF 和序列化器 51 将从闪速存储器 42 读取的数据输送到页面缓冲器 45 、读寄存器 48 和纠错电路 49 。纠错电路 49 校正存储在页面缓冲器 45 中的数据的差错。从页面缓冲器 45 中输出的纠错数据和从读寄存器 48 中输出的数据被输送到 S/P 和 P/S IF 块 43 ，然后通过串行接口 11 输送到记录器/播放器 1 的 CPU 2 中。

为了保护写在闪速存储器 42 中的内容(以 ATRAC 3 格式压缩的音频数据(ATRAC 3 数据))的版权，记录器/播放器 1 的安全块 3 和存储卡 40 的安全块 52 协同对该内容进行加密。安全块 52 具有缓冲存储器 53 、DES 加密电路 54 和非易失性存储器 55 等。

如附图 2 所示，配置 ROM 50 设置在控制块 41 中。配置 ROM 50 存储存储卡 40 的版本信息和各种类型的属性。存储卡 40 具有可由用户操作的写保护开关 60 。当将开关 60 放在写保护位置时，即使记录器/播放器 1 给闪速存储器 42 发送擦除指令，存储在闪速存储器 42 中的数据也禁止被擦除。当开关 60 放在非写保护位置时，可擦除存储在闪速存储器 42 中数据。振荡器 61 产生作为用于在存储卡 40 中执行的处理的时间基准的时钟信号。

存储卡 40 的安全块 52 具有许多验证密钥和存储卡专用存储密钥。非易失性存储器 55 存储不能从安全块 52 的外部存取的解密或存储密钥。安全块 52 具有随机数产生电路。安全块 52 能够验证记录器/播放器 1(其可以形成应用预定数据格式的专用系统)并与其共享对话密钥。应用对话密钥对用于加密 ATRAC 3 数据的内容密钥进行加密，并在记录器/播放器 1 和存储卡 40 之间传送。与存储卡 40 的安全块 52 相同，记录器/播放器 1 的安全块 3 具有设备

专用存储密钥。当内容已被加密并存储在闪速存储器 42 中时，应用存储密钥对相应的内容密钥进行加密，并与加密的内容一起存储。

附图 3 所示为没有加密功能的存储卡 40'。换句话说，存储卡 40'是非安全型存储卡。与附图 2 中所示的存储卡 40 不同的是，存储卡 40'并不包括安全块 52 。存储卡 40'的其它结构与存储卡 40 结构基本相同。此外，存储卡 40'的尺寸和形状也可与存储卡 40 的尺寸和形状都相同。由于在附图 1 中所示的记录器/播放器 1 是一种安全型的记录器，因此记录器/播放器 1 和存储卡 40 相互验证，并且在它们之间传递密钥。当将附图 3 中所示的存储卡 40'连接到记录器/播放器 1 时，记录器/播放器 1 测定存储卡 40'是非安全型的存储卡，并且记录器/播放器 1 不能使用这种非安全型的存储卡。

有几种方法可供记录器/播放器 1 测定所连接的存储卡的类型。作为一个实例，当将存储卡 40'连接到记录器/播放器 1 时，从记录器/播放器 1 将一密钥发送到存储卡 40'，以便验证它。由于存储卡 40'并不给记录器/播放器 1 发送正确的响应信号，因此，在超出时间期间后记录器/播放器 1 确定存储卡 40'不属于安全型存储卡。作为另一个实例中，当将存储卡 40 或 40'连接到记录器/播放器 1 时，表示存储卡是否是安全型的存储卡的识别信息可以记录在存储卡的预定区(引导区)中。一旦读取这种识别信息，记录器/播放器 1 确定所连接的存储卡的类型。

除了如附图 1 所示的记录器/播放器 1 外，依据本发明还提出一种能够应用非安全型的存储卡 40'的单元。一个实例是一种数字“手持摄像机(palm-corder)”，其将应用电荷耦合装置(CCD)照相机照的图片信息记录到存储卡 40'，并再现由此形成的图片。如下文将要描述，依据本发明的一个实施例，为增强存储卡 40 的兼容性，可以这样构造非安全型设备(比如数字手持摄像机)：使其能够成应用存储卡 40 记录和再现数据。换句话说，如上文所述，S/P 和 P/S IF 块 43 具有将用于闪速存储器 42 的指令和数据和用于安全块 52 的指令和数据分离的功能。

依据一个实施例，当应用盘形记录媒体时，存储卡 40'和 40 应用个人计算机的文件分配表(FAT)文件系统存储数据。闪速存储器 42 包括初始装载程序(IPL)区、 FAT 区和根目录区。 IPL 区存储初始装入到记录器/播放器 1 的存储器的程序的地址。此外， IPL 区存储闪速存储器 42 的各种信息。 FAT 区存储关于在闪速存储器 42 中的存储块的数据。换句话说， FAT 区存储表

示没有使用的块、下一块编号、坏块以及最后的块的值。根目录区存储目录项(文件属性、更新日期(年、月和日)、开始簇、文件大小等)。

除了以存储卡 40'和 40 的格式定义的文件管理系统外，也可以定义用于乐曲文件的文件管理信息(曲目信息管理文件)。应用存储卡 40'和 40 的用户块将曲目信息管理文件存储在闪速存储器 42 中。因此，即使存储卡 40'和 40 的 FAT 被破坏，该文件也能够恢复。

通过 CPU 2 创建曲目信息管理文件。当给记录器/播放器 1 通电时，CPU 2 确定存储卡 40'和 40 是否已经与记录器/播放器 1 连接。当存储卡 40'和 40 已经与记录器/播放器 1 连接时，CPU 2 读取闪速存储器 42 的引导块。依据引导块的识别信息，CPU 2 确定所连接的存储卡是否是安全型的存储卡。

如果连接了存储卡 40(即，安全型)，则 CPU 2 执行验证步骤。将从存储卡 40 中读取的其它数据存储在由 CPU 2 管理的一个存储器(未示)中。在发货之前在还没有使用的存储卡 40'和 40 的闪速存储器 42 中写入 FAT 和路线方向。当记录数据时，创建曲目信息管理文件。在 CPU 2 验证存储卡 40 之后，记录器/播放器 1 记录或再现加密的 ATRAC 3 数据文件。

当记录数据时，给 CPU 2 发送与操作按键 4 的操作相对应的记录指令。用编码器/解码器 7 压缩输入的音频数据。用安全块 3 对从编码器/解码器 7 接收的 ATRAC 3 数据进行加密。CPU 2 将经加密的 ATRAC 3 数据存储到存储卡 40 的闪速存储器 42 。此后，更新 FAT 和曲目信息管理文件。每当更新文件时(即，在记录音频数据后)，都可以将 FAT 和曲目信息管理文件重新写入到由 CPU 2 控制的存储器中。当存储卡 40 是与记录器/播放器 1 分离的或记录器/播放器 1 没有通电时，将最后的 FAT 和曲目信息管理文件从该存储器输送到存储卡 40 的闪速存储器 42 。在这种情况下，只要已经记录了音频数据，就可以重新改写存储在闪速存储器 42 中的 FAT 和曲目信息管理文件。当编辑了数据时，更新曲目信息管理文件的内容。

附图 4 所示为计算机系统的文件系统处理分层结构的示意图，该计算机系统应用存储卡 40'和 40 作为存储媒体。如附图所示，顶层是应用程序处理层。应用程序处理层之后为文件管理处理层、逻辑地址管理层、物理地址管理层和闪速存储器存取层。文件管理处理层是 FAT 文件系统。物理地址被指到存储卡 40'和 40 中的闪速存储器 42 的每个块。在闪速存储器 42 的块和其物理地址之间的关系并不改变。逻辑地址是对在文件管理处理层中进行逻辑

处理的地址。

附图 5 所示为在存储卡 40'和 40 的闪速存储器 42 中处理的数据的物理结构。在闪速存储器 42 中，将数据单元(称为段)划分为预定数目的块(固定长度)。将一块又划分为预定数目的页(固定长度)。在闪速存储器 42 中，一次擦除一块的数据。一次将一页数据写入闪速存储器 42 中或一次从闪速存储器 42 中读取一页的数据。每个块的大小相同。同样地每个页的大小也相同。一块包括第 0 页到第 m 页。一块的存储容量为 8KB(千字节)或 16KB，而一页的存储容量为 512B(比特)。当一块的存储容量为 8KB 时，闪速存储器 42 的总的存储容量为 4MB(512 块)或 8MB(1024 块)。如果一块的存储容量为 16KB，则闪速存储器 42 的总的存储容量为 16MB(1024 块)、32MB(2048 块)或 64MB(4096 块)。

一页包括 512 字节的数据部分和 16 字节的冗余部分。冗余部分的起始 3 个字节是改写部分，只要数据被更新该改写部分就重写。该起始 3 字节依次包含块状态区、页状态区和更新状态区。冗余部分的其它 13 字节是取决于数据部分的内容的固定数据。该 13 字节包含有管理标志区(1 字节)、逻辑地址区(2 字节)、格式预留区(5 字节)、离散信息纠错码(ECC)区(2 字节)和数据 ECC 区(3 字节)。离散信息 ECC 区包含用于管理标志区、逻辑地址区和格式预留区的纠错处理的冗余数据。数据 ECC 区包含用于对在 512 字节数据部分中的数据进行纠错处理的冗余数据。

管理标志区包含系统标志(1：用户块，0：引导块)、转换表标志(1：无效，0：表块)、禁止复制标志(1：允许复制，0：不允许复制)和访问许可标志(1：自由，0：读保护)。

开始的两个块(块 0 和 1)为引导块。块 1 是块 0 的备份。引导块是在存储卡 40'和 40 中有效的顶部块。当将存储卡 40'和 40 连接到记录器/播放器 1 时，首先访问引导块。其它块为用户块。引导块的第 0 页包含首标(header)区、系统入口区和引导和属性信息区。引导块的第 1 页包含被禁止的块数据区。引导块的第 2 页包含 CIS(卡信息结构)/IDI(识别驱动信息)区。

附图 6 所示为引导块的第 0、1 和 2 页的格式。引导块的首标区(368 字节)存储引导块的引导块 ID、格式的版本和合法入口数目。系统入口(48 字节)存储被禁止的块数据的起始位置及其数据大小和数据类型、CIS/IDI 的数据开始位置及其数据大小和数据类型。引导和属性信息包含存储卡的类型(只

读型、可重写型或混合型)、块大小、块数目、总块数、安全/非安全型、卡的制造数据(制造日期)等。

附图 7 所示为在附图 6 中所示的引导和属性信息(96 字节)的结构。引导和属性信息包含存储卡的等级、类型(只读型、可读写型或这两种类型的混合型，等)、块大小、块数目、总块数、安全/非安全型、卡的制造数据(制造日期：年、月、日)等。记录器/播放器 1 确定存储卡是否是一种应用安全信息(一个字节)的安全型存储卡。在附图 7 中，(*1)表示当连接存储卡时记录器/播放器 1 读取和校验的数据项，(*2)表示生产/质量管理数据项。

可以理解的是，每当重写存储在闪速存储器 42 中的数据时，闪速存储器 42 的绝缘膜就会老化。因此，存储卡 40'和 40 的使用寿命受闪速存储器 42 重写次数的限制。因此，最好防止对闪速存储器 42 的特定区域(块)的重复存取。因此，当重写存储在特定物理地址的数据时，不将所更新的数据写到相同的块中。而是将更新的数据写到还没有使用过的块中。因此，在更新数据后，物理地址和逻辑地址之间的关系也改变了。当进行这种处理时(称为交换过程)，就防止了对相同的块进行重复存取。因此，延长了闪速存储器 42 的使用寿命。

由于逻辑地址与写到块中的数据的相对应，因此，即使将更新的数据物理地移动到另外一块中，在 FAT 中仍然能够保持相同的逻辑地址。交换过程改变了在逻辑地址和物理地址之间的关系。因此，当进行这种交换处理时，改变了将逻辑地址变换为物理地址的转换表。参考这个转换表就可以得到与由 FAT 指定的逻辑地址相对应的物理地址。因此，可以应用相同的逻辑地址正确地访问更新的数据。

由 CPU 2 将逻辑－物理地址转换表存储在随机存取存储器(RAM)中。然而，当这种 RAM 的存储容量很小时，可以将这种逻辑－物理地址转换表存储在闪速存储器 42 中。这个表实质上是将升序排列的逻辑地址(2 字节)与物理地址(2 字节)对应起来。由于闪速存储器 42 的最大存储容量是 128MB(8192 块)，因此能够表示 2 字节的 8192 个地址。此外，一段一段地管理逻辑－物理地址转换表。这种逻辑－物理地址转换表的大小与闪速存储器 42 的存储容量成比例。如果闪速存储器 42 的存储容量是 8MB(2 段)，可以将对应于 2 段的 2 页用于逻辑－物理地址转换表。如果将逻辑－物理地址转换表存储在闪速存储器 42 中，每页的冗余部分的管理标志的一个位表示一相关的块是

否已经存储在逻辑－物理地址转换表中。

接着，下文进一步描述安全保护功能。首先，参考附图 8A 和 8B，描述在密钥和内容之间的关系。存储在闪速存储器 42 中的每个乐曲(或歌曲)称为一个曲目(track)。附图 8A 所示为存储在闪速存储器 42 中的一个曲目。如附图 8A 所示，每个曲目包括密钥区(首标区)101。应用存储卡专用存储密钥 Kstm 对为加密音频数据的每个曲目(标题)创建的内容密钥 CK 进行加密，并将所得到的结果数据存储在密钥区 101 中。DES 是用于对内容密钥 CK 和存储密钥 Kstm 进行加密处理的。DES(Kstm, CK)表示应用存储密钥 Kstm 对内容密钥 CK 进行加密。最好，编码值具有 64 位，该 64 位包括 56 位数据和用于由循环冗余校验(CRC)检错的 8 位。

每个曲目划分为片段 102。每个片段记录一个片段密钥 PK。如图所示，在附图 8A 中所示曲目仅包括一个片段 102。片段 102 是一系列的块 103(每块 16KB)。每个块 103 存储一个块籽数(seed)BK-SEED 和初始矢量 INV。片段密钥 PK 与内容密钥 CK 配对，以便创建用于对内容加密的块密钥 BK。换句话说，BK = DES(CK(+)PK, BK-SEED)(56 位 + 8 位)(这里(+)表示异或运算)。初始矢量 INT 是对块进行加密/解密处理的初始值。

附图 8B 涉及在记录器/播放器 1 中的内容数据。对内容的每个曲目的内容密钥 CK 进行解密，然后对所得到的结果应用记录器专用存储密钥 Kstd 进行再次加密。将再次加密后的数据存储在密钥区 111 中。换句话说，以 IDES(Kstm, CK)(56 位 + 8 位)表示解密过程，而以 DES(Kstd, CK)(56 位 + 8 位)表示再加密过程。对内容的每个片段 112 记录用于建立块密钥 BK 的片段密钥 PK。片段 112 的每个块 113 存储块籽数 BK-SEED 和初始矢量 INV。与存储卡相同，块密钥 BK 表示为 BK = DES(CK(+)PK, BK-SEED)(56 位 + 8 位)。

对存储卡 40 的写操作

下文将参考附图 9 描述可以应用在记录器/播放器 1 的记录(写)操作中的加密处理。为简洁，在附图 9 中以相同标号表示与在附图 1 中相同的部分，并且省略对它们的描述。此外，在附图 9 中省去了接口 11、总线 16 和控制块 41(通过它们在记录器/播放器 1 的部件和存储卡 40 之间传输数据和指令)，以使下面处理的解释变得简单。在附图 9 中，SeK 是在记录器/播放器 1 和存储卡 40 经过相互验证后、在它们之间共享的对话密钥。在附图 9 中，

参考标号 10'表示在数字输入端 10 输入的数字音频信号的源和 CD 。

当存储卡 40 连接到记录器/播放器 1 时，记录器/播放器 1 通过使用在引导区中的识别信息来确定存储卡 40 是否是安全型存储卡。由于存储卡 40 是安全型存储卡，所以记录器/播放器 1 和存储卡 40 要相互验证。

下文将参考附图 10 对在记录器/播放器 1 和存储卡 40 之间的相互验证的过程进行描述。

在将写请求信号从记录器/播放器 1 发送到存储卡 40 后，正如参考附图 10 下面进一步作出的详细描述那样，记录器/播放器 1 和存储卡 40 再次进行相互验证。如果根据相互识别过程记录器/播放器 1 和存储卡 40 彼此验证为合法的，则如参考附图 11 进一步描述的那样，执行密钥写过程。否则，终止写操作。在完成写操作后，对音频数据加密，并由 CPU 2 通过接口 11 将其写入到存储卡 40 中。

参考附图 9，记录器/播放器 1 对每个要写的数据(乐曲)的每个曲目产生一随机数，并依据每个随机数创建对应的内容密钥 CK 。记录器/播放器 1 的安全块 3 应用对话密钥 SeK 对内容密钥 CK 进行加密。记录器/播放器 1 将经加密的内容密钥 CK 输出到存储卡 40 中。在存储卡 40 中的安全单元 52 的 DES 加密/解密电路对经过加密的内容密钥 CK 进行解密，并应用来自存储器 55 的存储密钥 Kstm 对经解密的内容密钥 CK 进行再次加密。存储卡 40 将经再次加密的 CK 输出到记录器/播放器 1(CPU 2)中。记录器/播放器 1(CPU 2)将再次加密的内容密钥 CK 设置在每个曲目的密钥区 111(如附图 8B 所示)中。记录器/播放器 1 针对每个曲目的每片段数据区 112(如附图 8B 所示)产生随机数，并依据每个随机数创建片段密钥 PK 。 CPU 2 将所创建的每个片段密钥 PK 设置在相应的片段数据区 112 中。

通过记录器/播放器 1 对每个片段数据区 112 的片段密钥 PK 和内容密钥 CK 进行 XOR(异或)操作，来产生临时密钥 TMK ，如下等式(1)所示。并不限于应用 XOR 函数来产生临时密钥 TMK 。也可以应用其它的函数运算符，比如简单的 AND(与)运算符。

$$TMK = PK \text{ XOR } CK \qquad (1)$$

记录器/播放器 1 对每个片段数据区 112 的每个块 113 产生一随机数，并依据每个随机数创建块籽数 BK-SEED 。此外，记录器/播放器 1(CPU 2)将所创建的块籽数 BK-SEED 设定在每个相应块 113 的适当位置。记录器/播放器

1 应用临时密钥 TMK 和块籽数 BK-SEED 通过等式(2)执行消息验证码(MAC)操作，以创建每个块 113 的块密钥 BK 。

$$BK = MAC(TMK, BK\text{-}SEED) \qquad (2)$$

除了 MAC 操作外，还可以通过应用 SHA-1(安全散列(Hash)算法)、RIPEMD-160 或其它的单向散列函数的输入密钥来进行处理以创建块密钥 BK 。这里，单向函数 f 定义一种函数，从该函数中容易由 x 计算 y = f(x)，但反过来从 y 就难以计算 x 。在“(应用密码学手册)Handbook of Applied Cryptography， CRC Press ”详细地描述了单向散列函数。

音频编码器/解码器 7 对从 CD10'输入到数字输入端 10 的数字音频信号或来自 A/D 转换器 9 的数字信号依据 ATRAC 3 格式进行压缩，该转换器 9 将输入到模拟输入端 8 中的模拟音频信号转换为数字信号。然后，安全块 3 通过应用块密钥 BK 以密码块链接(CBC)模式对压缩的音频数据进行加密，该 CBC 模式是在联邦信息处理标准(FIPS)PUB 81(数据加密标准运行模式(DES MODES OF OPERATION))中规定的一种数据加密模式。

记录器/播放器 1 将首标加入到经加密的音频数据中，并将所得到的结果输出到存储卡 40 中。存储卡 40 将经加密的音频数据和首标写入到闪速存储器 42 中。这里，完成了将音频数据从记录器/播放器 1 写到存储卡 40 中的过程。

附图 10 所示为在记录器/播放器 1(设备)和存储卡 40(存储卡)之间进行验证的过程。在步骤 S1 中，在存储卡 40 中的安全块 52 的随机数发生器产生随机数 Rm，并将随机数 Rm 和存储卡 40 的序号 ID 发送到记录器/播放器 1 中。

在步骤 S2 中，记录器/播放器 1 接收 Rm 和 ID，并根据如下的关系产生验证密钥 IKj:IKj = MAC(MKj, ID)，这里 MKj 是存储在安全块 3 中的一个主密钥。记录器/播放器 1 产生随机数 Rm，并应用验证密钥创建信息验证码 MAC_A(信息验证码)，即 MAC(IK, Rd//Rm//ID)。此后，记录器/播放器 1 产生随机数 Sd，并将 Rd//Sd//MAC_A/j 发送到存储卡 40 中。

在步骤 S3 中，存储卡 40 接收 Rd//Sd//MAC_A//j 数据，从安全块 52 中找到与 j 对应的验证密钥 IKj，并通过验证密钥 Ikj 应用 Rd 、Rm 和 ID 计算 MAC_B。当所计算的 MAC_B 与所接收的 MAC_A 相等时，存储卡 40 确认记录器/播放器 1 是合法(即，被授权)。在步骤 S4 中，存储卡 40 创建 MAC_C =

MAC(IKj， Rm//Rd)，并产生随机数 Sm 。此后，存储卡 40 将 Sm//MAC_C 发送到记录器/播放器 1 。

在步骤 S5 中，记录器/播放器 1 从存储卡 40 中接收 Sm//MAC_C 。记录器/播放器 1 应用 Ikj 、Rm 和 Rd 计算 MAC_D 。当所计算的 MAC_D 与所接收的 MAC_C 相等时，记录器/播放器 1 确认存储卡 40 是合法(即，被授权)。在步骤 S6 中，记录器/播放器 1 指定 MAC(IKj, Rm//Rd)作为对话密钥 SeK 。在步骤 S7 中，存储卡 40 指定 MAC(IKj, Rm//Rd)作为对话密钥 SeK 。当记录器/播放器 1 和存储卡 40 进行相互验证时，它们之间共享对话密钥 SeK 。只要验证成功就创建对话密钥 SeK 。

附图 11 所示为在记录器/播放器 1(设备)将音频数据记录到存储卡 40(存储卡)的闪速存储器 42 中的情况下写密钥的过程。在步骤 S11 中，记录器/播放器 1 对内容的每个曲目都产生随机数，并创建内容密钥 CK 。在步骤 S12 中，记录器/播放器 1 应用对话密钥 SeK 对内容密钥 CK 进行加密，并将经加密的 DES(SeK, CK)发送到存储卡 40 中。

在步骤 S13 中，存储卡 40 从记录器/播放器 1 中接收数据 DES(SeK, CK)，并用对话密钥 SeK 对内容密钥 CK 进行解密。解密过程表示为 IDES(SeK, DES(SeK, CK))。在步骤 S14 中，存储卡 40 用来自存储器 55 的存储密钥 Kstm 对经解密的内容密钥 CK 进行再次加密，并将再次加密的内容密钥 DES(Kstm, CK)输送到记录器/播放器 1 中。

在步骤 S15 中，记录器/播放器 1 将再次加密的内容密钥 CK 放在管理相应片段数据区 112 的密钥区 111 中，并进行格式化处理，以将再次加密的内容密钥 CK 和内容记录在存储卡 40 的闪速存储器 42 中。为了对内容进行加密，如附图 9 和上述等式 11 所示对内容密钥 CK 和片段密钥 PK 进行异或运算(XOR，或可替换地， AND)。 XOR 运算的结果为临时密钥 TMK 。临时密钥 TMK 仅存储在安全块 3 中。因此，并不能从安全块 3 以外访问临时密钥 TMK 。在每个块 113 的开始，产生随机数作为块籽数 BK-SEED 。随机数存储在每个片段数据区 112 中。记录器/播放器 1 应用临时密钥 TMK 对块籽数 BK-SEED 进行加密，以得到块密钥 BK 。换句话说，得到关系 BK = (CK(+)PK, BK-SEED)。将块密钥 BK 仅存储在安全块 3 中。因此，并不能从安全块 3 以外访问块密钥 BK 。

在步骤 S16 中，记录器/播放器 1 应用块密钥 BK 逐块地加密在每个片段

数据区 112 中的数据，并将经加密的数据和在密钥区 111 中的数据发送到存储卡 40 中。在步骤 S17 中，存储卡 40 将从记录器/播放器 1 接收到的经加密的数据和在密钥区 111 中的数据(首标数据)记录到闪速存储器 42 中。

对存储卡 40 的读操作

下面参考附图 12 解释用在记录器/播放器 1 的再现(读取)操作中的解密过程。在附图 12 中，为简洁起见，省去对与在附图 1 中类似的标号所表示的部分类似的那些部分的描述。此外，在附图 12 中省去了接口 11 、总线 16 和控制块 41(通过它们在记录器/播放器 1 的部件和存储卡 40 之间传输数据和指令)，以使解释下面的方法变得简单。

从记录器/播放器 1 中将指定所需的数据(乐曲)的曲目的读请求信号发送到存储卡 40 中。如上文参考附图 10 所述，记录器/播放器 1 和存储卡 40 进行相互验证操作。如果依据相互识别过程记录器/播放器 1 和存储卡 40 彼此认为对方为合法的，则如上文参考附图 11 所描述那样执行密钥写过程。否则，终止读操作。在完成密钥写操作后， CPU 2 从存储卡 40 中经将经加密的音频数据读入到记录器/播放器 1 中。

由于在存储卡 40 和记录器/播放器 1 之间进行相互识别，因此，仅当存储卡 40 和记录器/播放器 1 彼此识别对方为合法时才能够应用正确的对话密钥 SeK 对经加密的内容密钥 CK 进行解密。因此，能够很容易地避免非法地应用音频数据。通过如上述的在附图 9 中所描述的写操作，写入已经在读取操作过程中读取的数据。在每个片段数据区 112 中设定片段密钥 PK 和内容密钥 CK ，并且应用在每个块 113 中的块籽数 BK-SEED 来将数据写到相应的片段数据区 102 以及从相应的片段数据区 102 中读取数据。在完成附图 10 中的步骤 S6 后，存储卡 40 和记录器/播放器 1 共享对话密钥 SeK 。从存储卡 40 中读取的音频数据的操作继续进行如下。

存储卡 40 指定在片段数据区 102(附图 8A)中与读请求信号对应的数据，并且输出在指定片段数据区 102 中来自块 103(附图 8A)的声音单元 SU 中的音频数据。存储卡 40 还读取音频数据的对应的密钥区 101(附图 8A)，并将其输出到记录器/播放器 1 中。

记录器/播放器 1 从在密钥区 101 中的数据中拾取经加密的内容密钥 CK ，并将其输出到存储卡 40 。在存储卡 40 中的安全块 52 的 DES 加密/解密电路 54 应用存储在存储器 55 中的存储密钥 Kstm 对经加密的内容密钥 CK

进行解密，并应用对话密钥 SeK 对经解密的内容密钥 CK 进行再次加密。

存储卡 40 将经再次加密的内容密钥 CK 输出到记录器/播放器 1 中。记录器/播放器 1 应用对话密钥 SeK 对来自存储卡 40 的经再次加密的内容密钥 CK 进行解密。然后，记录器/播放器 1 对经解密的内容密钥 CK 和来自每个片段数据区 102 中的数据的片段密钥 PK 实行 XOR 操作，以便依据等式(3)得到临时密钥 TMK 。

$$TMK = PK \text{ XOR } CK \qquad (3)$$

记录器/播放器 1 在每个片段数据区 102 中使用临时密钥 TMK 和块籽数 BK-SEED，以执行如在下式(4)中所示的 MAC 运算，以得到块密钥 BK 。如下面所述为每个块 103 都求出块密钥 BK 。

$$BK = MAC(TMK, BK\text{-}SEED) \qquad (4)$$

记录器/播放器 1 的安全块 3 通过应用块密钥 BK 对音频数据进行解密。更具体地说，应用分别求出的块密钥 BK 对每个块 103 的音频数据进行解密。此外，在与用于加密相同的 16KB 块 103 中进行解密。音频编码器/解码器 7 依据 ATRAC 3 系统对经加密的音频数据进行展开，并通过数字输出端 14 输出解码信号，或 D/A 转换器 12 将数字音频信号转换为模拟信号，并通过模拟输出端 13 输出结果。作为一种变型，将来自安全块 3 的 ATRAC 3 音频数据通过输出端 15 输出。音频编码器/解码器 7 以声音单元 SU 展开音频数据。

附图 13 所示为当记录器/播放器 1 再现存储在存储卡 40 的闪速存储器 42 中的音频曲目时的解密过程。如附图 9 至 11 所示的写操作，在记录器/播放器 1 和存储卡 40 相互验证后它们之间共享对话密钥 SeK 。

在步骤 S21 中，记录器/播放器 1(设备)从存储卡 40(存储卡)中读取数据，得到以存储密钥 Kstm 加密的内容密钥 CK(即， DES(Kstm, CK))和经加密的内容(所需曲目的一个或多个片段数据区 102)。此后，记录器/播放器 1 将以存储密钥 Kstm 加密的内容密钥 CK 输送到存储卡 40 中。

在步骤 S22 中，存储卡 40 应用存储密钥 Kstm 对内容密钥 CK 进行解密(即， IDES(Kstm, DES(Kstm, CK)))。在步骤 S23 中，存储卡 40 应用对话密钥 SeK 对经解密的内容密钥进行加密，并将 DES(SeK, CK)输送到记录器/播放器 1 中。

在步骤 S24 中，记录器/播放器 1 应用对话密钥 SeK 对内容密钥进行解密。在步骤 S25 中，记录器/播放器 1 应用解密的内容密钥 CK 、片段密钥

PK 和块籽数 BK-SEED 创建块密钥 BK 。在步骤 S26 中，记录器/播放器 1 应用块密钥逐块地对每个经加密的片段数据区 102 进行解密。音频编码器/解码器 7 对经解密的音频数据进行解码。

参考在附图 2 中所示的接口 11，附图 14 说明了从存储卡 40 中读取数据的时序图。在除状态 0(初始状态)以外的其它状态，通过时钟线 SCK 发送用于数据同步的时钟信号。当在记录器/播放器 1 和存储卡 40 之间发送或接收数据时，状态线 SBS 的信号电平为低电平。初始状态可以称为状态 0(初始状态)。在时序 t31 时，记录器/播放器 1 使状态线 SBS 的信号电平变为高电平(状态 1)。

当状态线 SBS 的信号电平为高电平时，存储卡 40(S/P 和 P/S IF 块 43)确定状态 0 已变为状态 1 。在状态 1 中，记录器/播放器 1 通过数据线 DIO 发送读指令给存储卡 40 。因此，存储卡 40 接收读指令。读指令是一种称为传输协议指令(TPC)的协议指令。正如下文所述，协议指令指定通信的内容和后续的数据长度。

在时序 t32，在发送指令后，状态线 SBS 的信号电平从高电平变到低电平。因此，状态 1 改变到状态 2 。在状态 2 中，执行由存储卡 40 接收的指令所表示的操作。实际上，从闪速存储器 42 中读取由读指令所指定的地址数据到页面缓冲器 45 。在执行该过程的同时，通过数据线 DIO 给记录器/播放器 1 发送忙(busy)信号(高电平)。

在时序 t33，在已经将数据从闪速存储器 42 中读到页面缓冲器 45 后，停止发送忙信号。给记录器/播放器 1 输出就绪(ready)信号(低电平)，该就绪信号表示存储卡 40 准备依据读指令发送数据。

当记录器/播放器 1 从存储卡 40 中接收到就绪信号时，记录器/播放器 1 确定存储卡 40 准备处理读指令。在时序 t34，记录器/播放器 1 使状态线 SBS 的信号电平变为高电平。换句话说，状态 2 变到状态 3 。

在状态 3 中，存储卡 40 通过数据线 DIO 将已经在状态 2 中读入到页面缓冲器 45 中的数据输出到记录器/播放器 1 。在时序 t35，在发送读数据后，记录器/播放器 1 停止通过时钟线 SCK 发送时钟信号。此外，记录器/播放器 1 使状态线 SBS 电平从高变到低。因此，状态 3 变为初始状态(状态 0)。

当在时序 t36 时比如由于在存储卡 40 中的状态改变导致应该执行中断时，存储卡 40 通过数据线 DIO 给记录器/播放器 1 发送中断信号。当在状态

0 中记录器/播放器 1 通过数据线 DIO 从存储卡 40 接收中断信号时，记录器/播放器 1 确定信号为中断信号，并执行与中断信号对应的处理。

附图 15 是一操作时序图，其将数据写到存储卡 40 的闪速存储器 42 中。在初始状态(状态 0)中，并不通过时钟线 SCK 发送时钟信号。在时序 t41 时，记录器/播放器 1 使状态线 SBS 的信号电平从低变到高。因此，状态 0 变到状态 1 。在状态 1 中，存储卡 40 准备接收指令。在时序 t41 时，通过数据线 DIO 将写指令发送到存储卡 40 中，并且存储卡 40 接收写指令。

在时序 t42 中，记录器/播放器 1 使状态线 SBS 的信号电平从高变到低。因此，状态 1 变到状态 2 。在状态 2 中，记录器/播放器 1 通过数据线 DIO 将写数据发送到存储卡 40 中，并且存储卡 40 将所接收的写数据存储在页面缓冲器 45 中。

在时序 t43 中，记录器/播放器 1 使状态线 SBS 的信号电平从低变到高。因此，状态 2 变到状态 3 。在状态 3 中，存储卡 40 将写数据写入闪速存储器 42 中，并且存储卡 40 通过数据线 DIO 给记录器/播放器 1 发送忙信号(高电平)，记录器/播放器 1 给存储卡 40 发送写指令。由于当前状态是状态 3 ，因此，记录器/播放器 1 确定从存储卡 40 接收的信号是状态信号。

在时序 t44 ，存储卡 40 停止输出忙信号，并给记录器/播放器 1 发送就绪信号(低电平)。当记录器/播放器 1 接收到就绪信号时，记录器/播放器 1 确定与写指令相对应的写操作已经完成，并停止发送时钟信号。此外，在时序 t45 ，记录器/播放器 1 使状态线 SBS 的电平从高变到低。因此，状态 3 返回到状态 0(初始状态)。

当记录器/播放器 1 在状态 0 中从存储卡 40 通过数据线 DIO 接收到高电平信号时，记录器/播放器 1 确定所接收的信号为中断信号。记录器/播放器 1 执行与所接收的中断信号相对应的操作。当存储卡 40 与记录器/播放器 1 分离时，存储卡 40 产生中断信号。

除了读操作和写操作外，在状态 1 中还发送指令。在状态 2 中还发送与指令对应的数据。

需注意的是，设置在记录器/播放器 1 和存储卡 40 之间的串行接口并不限于如上所述的接口 11 。换句话说，可以使用各种形式的串行接口。

附图 16 为通过串行接口的数据线 DIO 发送的协议指令(TPC 码)的实例。每个协议指令的数据长度为一个字节。在附图 16 中，每个协议指令以

十六进制(带有后缀 h)和十进制(0 和 1)表示。此外，每个协议指令的定义都用于非安全型存储卡 40'(参见附图 3)和安全型存储卡 40(参见附图 2)。在附图 16 中，R 和 W 分别表示读类型的协议指令和写类型的协议指令。如上所述，由于在状态 1 中发送指令，而在状态 2 中发送数据，因此，示出了与每个协议指令对应的数据长度(以字节表示)。

现在描述每个协议指令 TPC 。

TPC = 2Dh 是对常规闪速存储器的存取指令(简单地称这个指令为存储器控制指令)。这个指令是页面数据读指令，并且对存储卡 40 和 40'是通用的。在该指令之后的数据长度为一页的数据长度(512 字节 + 2 字节(CRC))。页面数据是从页面缓冲器 45 中读取的。

TPC = D2h 是寄存器控制指令。这个指令是页面数据写指令。在该指令之后的数据长度为一页的数据长度(512 字节 + 2 字节(CRC))。将页面数据写入页面缓冲器 45 。

TPC = 4Bh 是寄存器控制指令。这个指令是对读寄存器 48 的读指令。在这个指令之后的数据长度为(31 字节 + 2 字节(CRC))。

TPC = B4h 是寄存器控制指令。这个指令是对写寄存器 46 的写指令。在该指令之后的数据长度为(31 字节 + 2 字节(CRC))。

TPC = 78h 是寄存器控制指令。这个指令是用于从读寄存器 48 读取一个字节的指令。在该指令之后的数据长度为(1 字节 + 2 字节(CRC))。

TPC = 87h 是寄存器控制指令。这个指令是用于改变指令寄存器 44 的访问范围的指令。在这个指令之后的数据长度为(4 字节 + 2 字节(CRC))。

TPC = 1Eh 是用于存储卡 40 的安全块 52 的状态寄存器的数据读取指令。然而，这个指令未对存储卡 40'定义。在该指令之后的数据的数据长度为(2 字节 + 2 字节(CRC))。专用于安全块 52 的指令称为安全指令。

TPC = E1h 是存储器控制指令。这个指令是设定与指令寄存器 44 对应的指令的指令。这个指令后的指令的级别比 TPC 指令的级别更低。因此，这个指令的数据长度为(1 字节 + 2 字节(CRC))。

TPC = 3Ch 对存储卡 40 的安全块 52 的安全数据读指令。然而，这个指令未对存储卡 40'定义。在该指令之后的数据的数据长度为(24 字节 + 2 字节(CRC))。

TPC = C3h 对存储卡 40 的安全块 52 的安全数据写指令。然而，这个指

令未对存储卡 40'定义。在该指令之后的数据的数据长度为(26 字节 + 2 字节(CRC))。

现在参考附图 17 和 18 。下面描述在 TPC = E1h 指令之前的指令(1 字节)。附图 17 说明了用于非安全型存储卡 40'。这些指令如下：

E1h = AAh : 块读指令

E1h = 55h : 块写指令

E1h = 33h : 块读/写取消指令

E1h = 99h : 块擦除指令

E1h = CCh : 存储器操作停止指令

E1h = 5Ah : 节电模式指令

E1h = C3h : 页面缓冲器清除指令

E1h = 3Ch : 存储器控制器复位指令

附图 18 说明了用于安全型存储卡 40 的指令。由于在附图 18 中所示的指令的定义(AAh 至 3CH)与在附图 17 中所示的指令的定义相同，因此省略对它们的说明。换句话说，这些指令是与存储卡 40 和 40'共同定义的存储器控制指令。在附图 18 中，指令(60h 至 83h)是专用于存储卡 40 进行加密过程(包括解密过程和验证过程)的安全指令。

如附图 17 和 18 所示，定义了存储卡 40 和 40'通用的存储器控制指令和专用于存储卡 40 的安全指令 TPC 。同样地，将这种关系应用到更低分层的指令中。换句话说，在更低级分层的指令中，定义公共存储器控制指令和安全指令。这种安全指令未对存储卡 40'定义。依据示例性的实施例，当 S/P 和 P/S IF 块 43 通过串行接口从记录器 1 接收指令时，存储卡 40 确定所接收的指令 TPC 是公共存储器控制指令还是安全指令。存储卡 40 根据所确定的结果将后续数据发送到对应的恰当的电路中。例如当所接收的指令是 TPC = E1h 指令，该指令后跟着另外一个指令，则存储卡 40 将指令发送到与在附图 18 中所示的指令定义所对应的适当的电路中。

附图 19 描述了对应于所接收的指令的选择数据要送到的电路的示意图。该结构设置在存储卡 40 的接口电路 43 中。通过数据线 DIO 从记录器 1 将数据输送到存储卡 40 中。通过延迟电路 150 将所接收的数据输送到切换电路 152 的端子“ a ”中。此外，将所接收的数据输送到检测电路 151 的输入端中。检测电路 151 依据协议指令的码值确定通过数据线 DIO 所接收的协

议指令(TPC)是存储器控制指令还是安全指令。依据所确定的结果控制切换电路 152 。延时电路 150 补偿检测电路 151 的检测时间。在 S/P 和 P/S IF 块 43 中通过硬件或软件实现这些结构元件。依据本实施例，由于将没有用于存储器控制指令的代码分配给安全指令，因此，检测电路 151 能够很容易地确定这两种指令的类型。

当检测电路 151 确定所接收的协议指令为存储器控制指令时，检测电路 151 的端子“ a ”连接到端子“ b ”。因此，通过检测电路 151 的端子“ a ”和“ b ”将存储器控制指令输送到页面缓冲器(例如在附图中所示的页面缓冲器 45 ，但为简明起见在附图 19 中省去了)、寄存器(例如在附图 2 中所示的寄存器 46 或 48)等等，以便控制闪速存储器 42 。将在存储器控制指令后的数据输送到页面缓冲器、寄存器等。可替换的是，通过检测电路 151 的端子“ a ”和“ b ”将数据从页面缓冲器、存储器等输送到记录器 1 。

当检测电路 151 确定所接收的协议指令为安全指令时，将检测电路 151 的端子“ a ”连接到端子“ c ”。通过检测电路 151 的端子“ a ”和“ c ”将安全指令输送到安全块 52 。将在安全指令后的数据输送到安全块 52 。通过检测电路 151 的端子“ a ”和“ c ”将数据从安全块 52 输送到记录器 1 。

当所接收的指令是协议指令(TPC = E1h)时，在该指令后为普通的存储器控制指令或安全指令。当检测电路 151 接收 TPC = E1h 协议指令时，检测电路 151 确定该指令后是控制指令还是安全指令。然后存储卡 40 依据所确定的结果控制切换电路 151 。当所接收的指令是除 TPC = E1h 协议指令外的其它指令，并且它随后为存储器控制指令或安全指令时，则存储卡 40 将数据发送到与该指令的码值相对应的适当电路中。

由于存储卡 40 具有用于确定所接收的指令是存储器控制指令还是安全指令的功能，所以存储卡 40 能够用于非安全型记录器。换句话说，非安全型记录器并不与存储卡 40 交换保密信息。非安全型记录仅将写/读存储器控制指令和将相应的数据发送到存储卡 40 中。如上所述，存储卡 40 确定从记录器所接收的指令是否是存储器控制指令，并将数据写入闪速存储器 42 或从闪速存储器 42 中读数据。因此，能够将数据写到存储卡 40 或从存储卡 40 中读数据。

依据上文所描述的实施例， DES 为优选的加密方法。但是，可以理解的是，作为其它变型也可以应用其它各种加密技术。

依据本发明，具有非易失性存储器和安全块的存储卡可以应用于安全型和非安全型数据处理设备(电子设备)，比如音频和/或视频记录器。因此，提高了安全型存储卡的兼容性。

此外，依据本发明，由于将未在数据处理设备和存储卡之间通信中使用的代码分配给安全操作的控制数据，因此相对于常规的非安全型存储卡实现了如上所指出的兼容性而无任何不利。换句话说，当采用非安全型电子设备时，该电子设备可以应用依据本发明的安全型存储卡。在将新的标识符加入到在电子设备和存储卡之间交换的数据并识别数据类型的一种方法中，除了需要新的标识符外，其它的电子设备不能使用。然而，应用本发明，并不存在这种问题，能够实现与常规的电子设备和常规的存储卡之间的兼容。

可以理解的是，所附权利要求覆盖在这里描述的所有的一般特征和特定特征、以及在本发明范围内的所有描述。

32

说 明 书 附 图

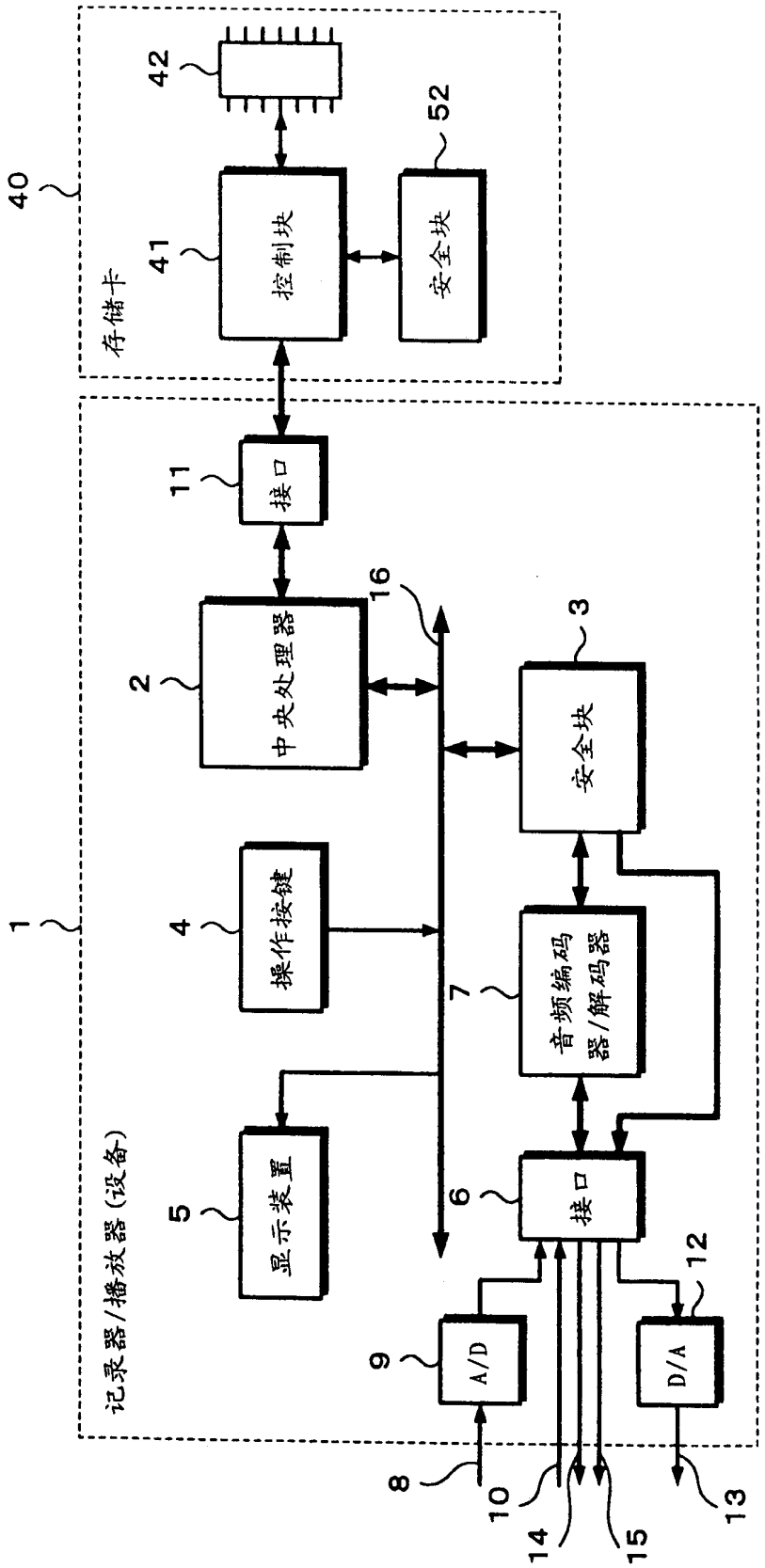

40
存储卡
42
41
控制块
52
安全块
1
记录器/播放器(设备)
11
接口
2
中央处理器
16
3
安全块
4
操作按键
7
音频编码器/解码器
5
显示装置
6
接口
12
9
A/D
D/A
8
10
14
15
13

图 1

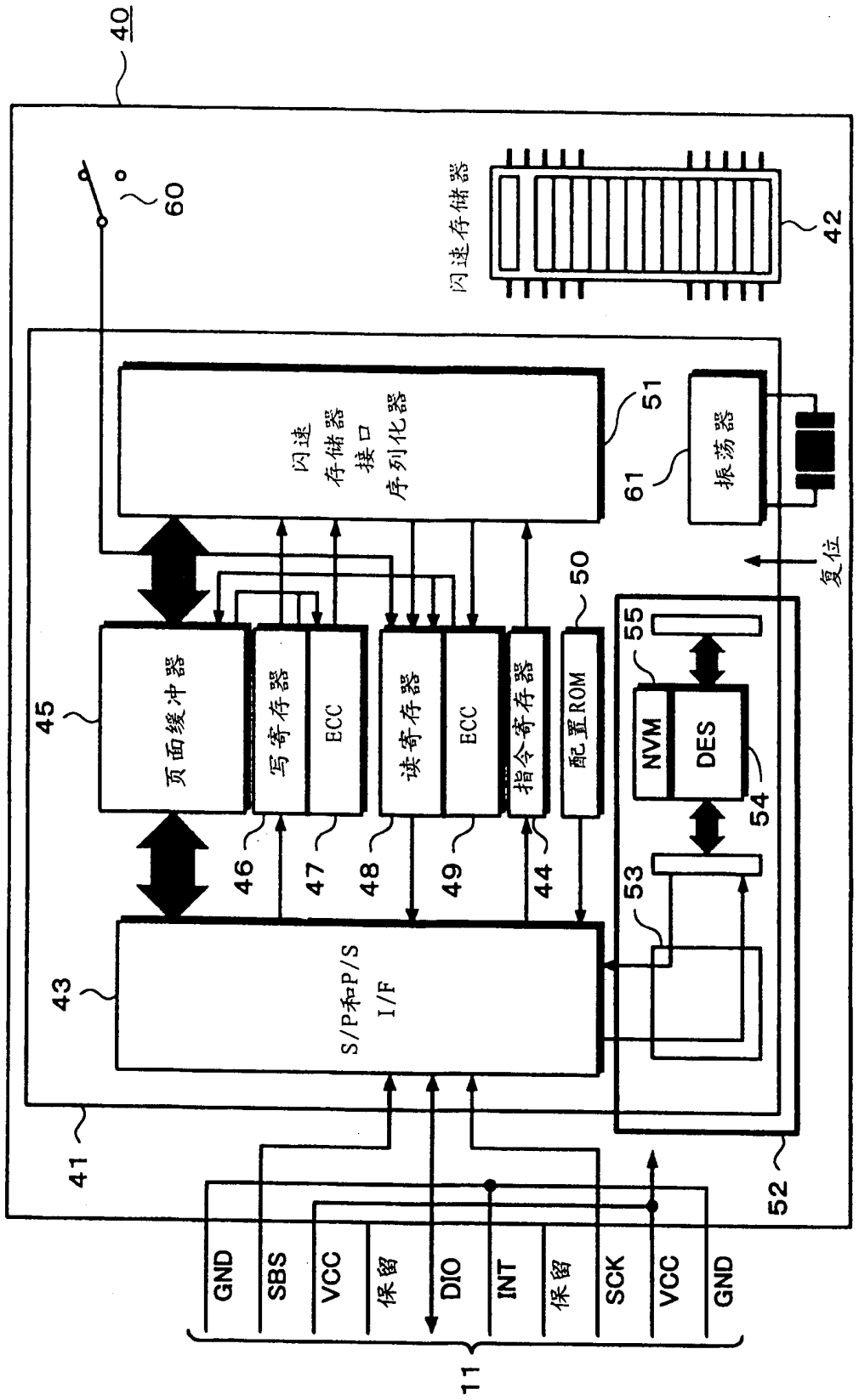

40
60
闪速存储器
42
闪速
存储器
接口
序列化器
51
61
振荡器
复位
50
55
NVM
DES
54
53
45
页面缓冲器
写寄存器
ECC
读寄存器
ECC
指令寄存器
配置ROM
46
47
48
49
44
43
S/P和P/S
I/F
41
52
GND
SBS
VCC
保留
DIO
INT
保留
SCK
VCC
GND
11

图 2

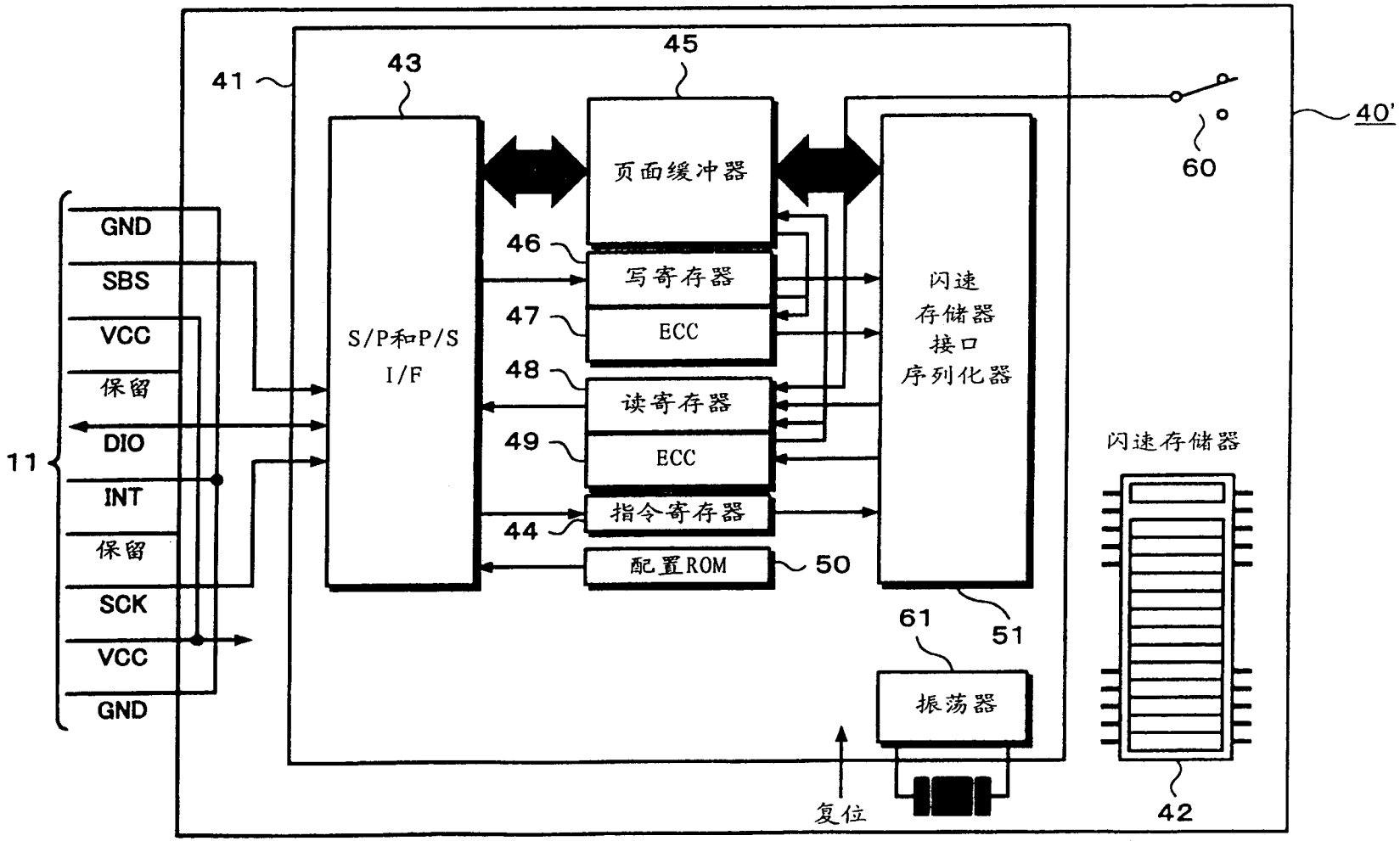
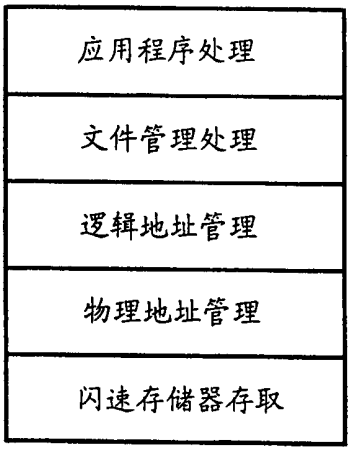

41
43
45
40'
60
页面缓冲器
GND
SBS
VCC
保留
DIO
INT
保留
SCK
VCC
GND
11
S/P和P/S
I/F
46
写寄存器
47
ECC
48
读寄存器
49
ECC
44
指令寄存器
配置ROM
50
闪速
存储器
接口
序列化器
51
61
振荡器
复位
闪速存储器
42

图 3



文件系统处理分级结构

图 4

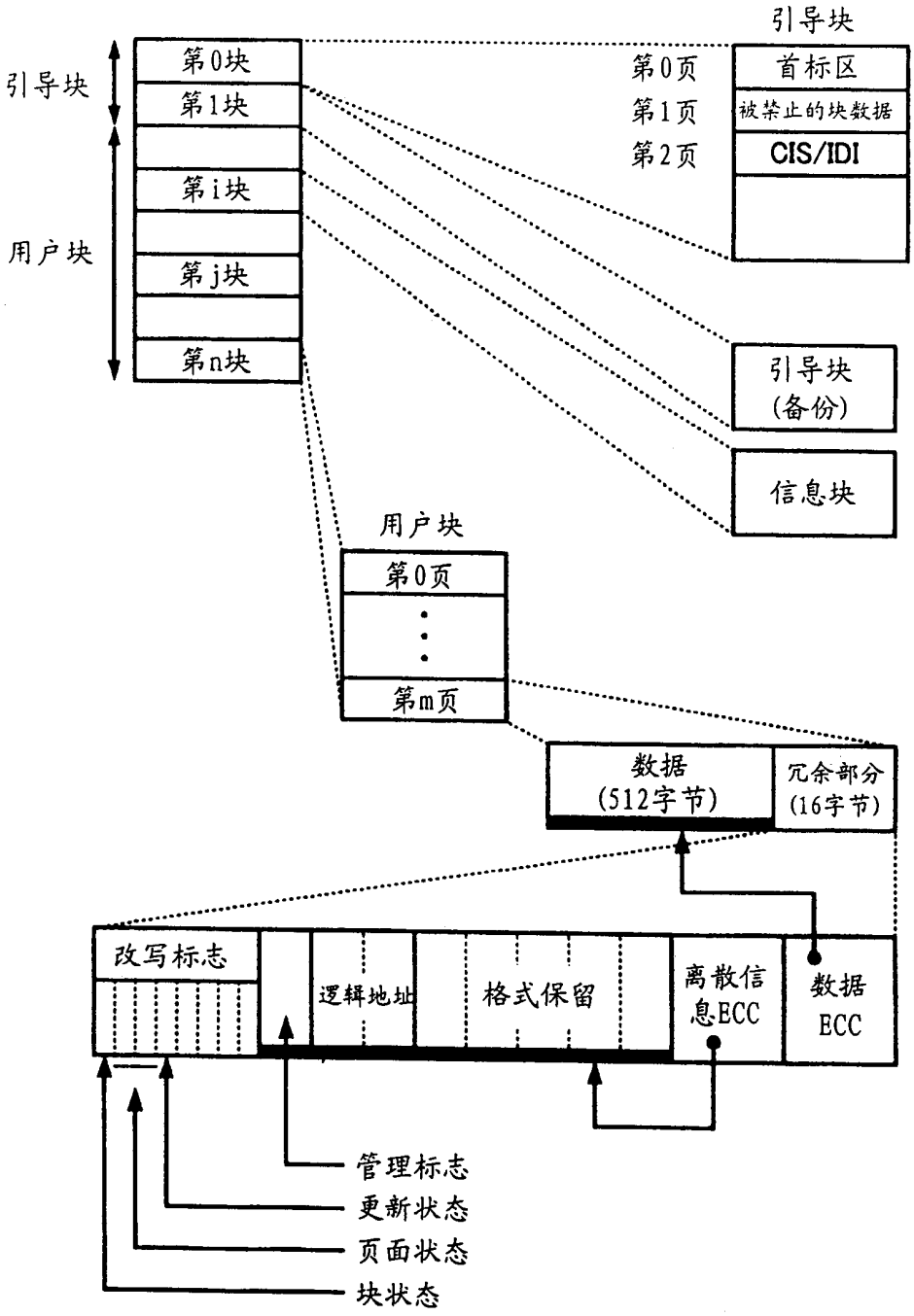

引导块
第0块
第1块
第i块
第j块
第n块
用户块
引导块
第0页
第1页
第2页
首标区
被禁止的块数据
CIS/IDI
引导块
(备份)
信息块
用户块
第0页
第m页
数据
(512字节)
冗余部分
(16字节)
改写标志
逻辑地址
格式保留
离散信息ECC
数据ECC
管理标志
更新状态
页面状态
块状态

图 5

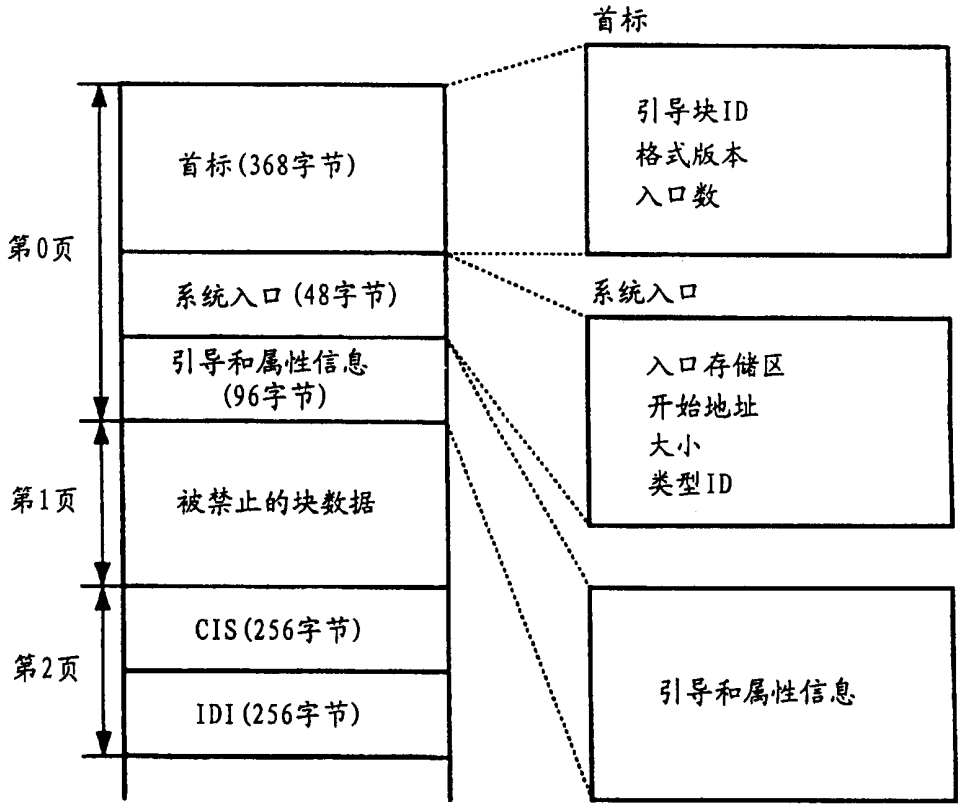

首标
引导块ID
格式版本
入口数
首标(368字节)
第0页
系统入口(48字节)
系统入口
引导和属性信息
(96字节)
入口存储区
开始地址
大小
类型ID
第1页
被禁止的块数据
CIS(256字节)
第2页
IDI(256字节)
引导和属性信息

图 6

		字节数	
MS等级	(*1)	1	1: 类型-1，其它预留
存储卡类型	(*1)	1	1: 只读 2: 读写 3: 混合型或其它预留
块大小	(*1)	2	块大小(以KB计) 16KB: 0x0010 8KB: 0x0008
块数	(*1)	2	块数目
块总数	(*1)	2	总块数目
页面大小		2	页面大小，512固定，0x0200
冗余部分大小		1	冗余部分大小=16字节: 0x10
安全类型	(*1)	1	
制造日期	(*2)	8	存储卡(硬)的制造日期 (日期和时间指定格式见下一页)
制造商区域	(*2)	4	用于市场管理比如序列号
MS装配制造商代码	(*2)	1	寄存器生产商代码
MS装配类型代码	(*2)	3	寄存器生产类型代码
存储器生产商代码		2	芯片制造商代码0: 未知
存储器设备代码		2	设备代码0: 未知
存储器大小		2	MB cs: 32兆位，闪速存储0x0004
格式预留		1	1: 其它预留
格式预留		1	1: 其它预留
VCC		1	VCC单元: 0.1V ex) 3.3V 0x21
VPP		1	VPP单元: 0.1V ex) 3.3V 0x21
控制器号		2	控制器芯片号
保留		14	
格式类型	(*1)	1	1: FAT，其它预留
应用		1	0: 一般目的，其它预留
零复位预留		5	
保留		35	

图 7

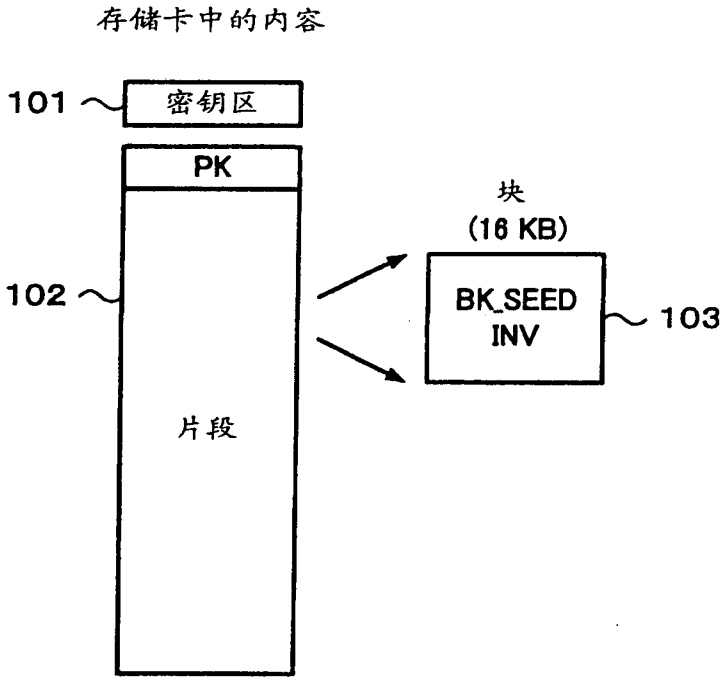

存储卡中的内容
101
密钥区
PK
102
片段
块
(16 KB)
BK_SEED
INV
103

图 8A

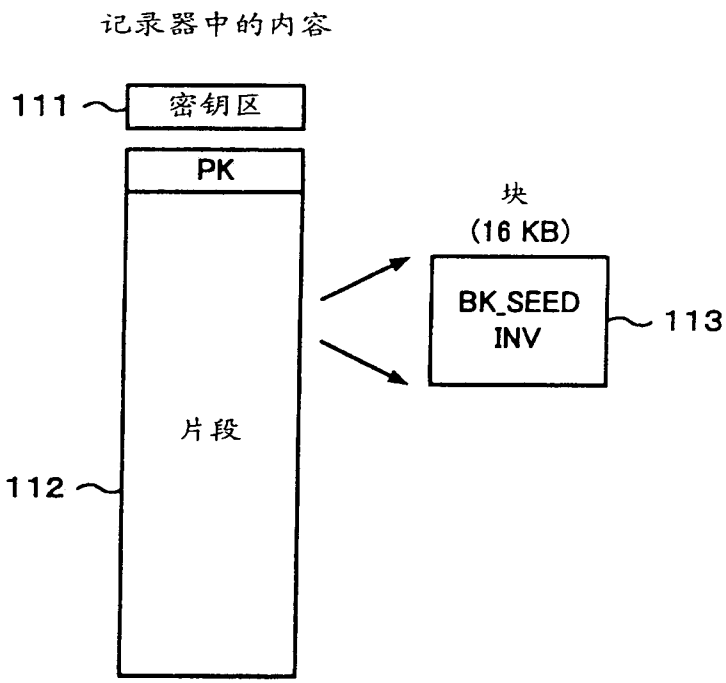

记录器中的内容
111
密钥区
PK
112
片段
块
(16 KB)
BK_SEED
INV
113

图 8B

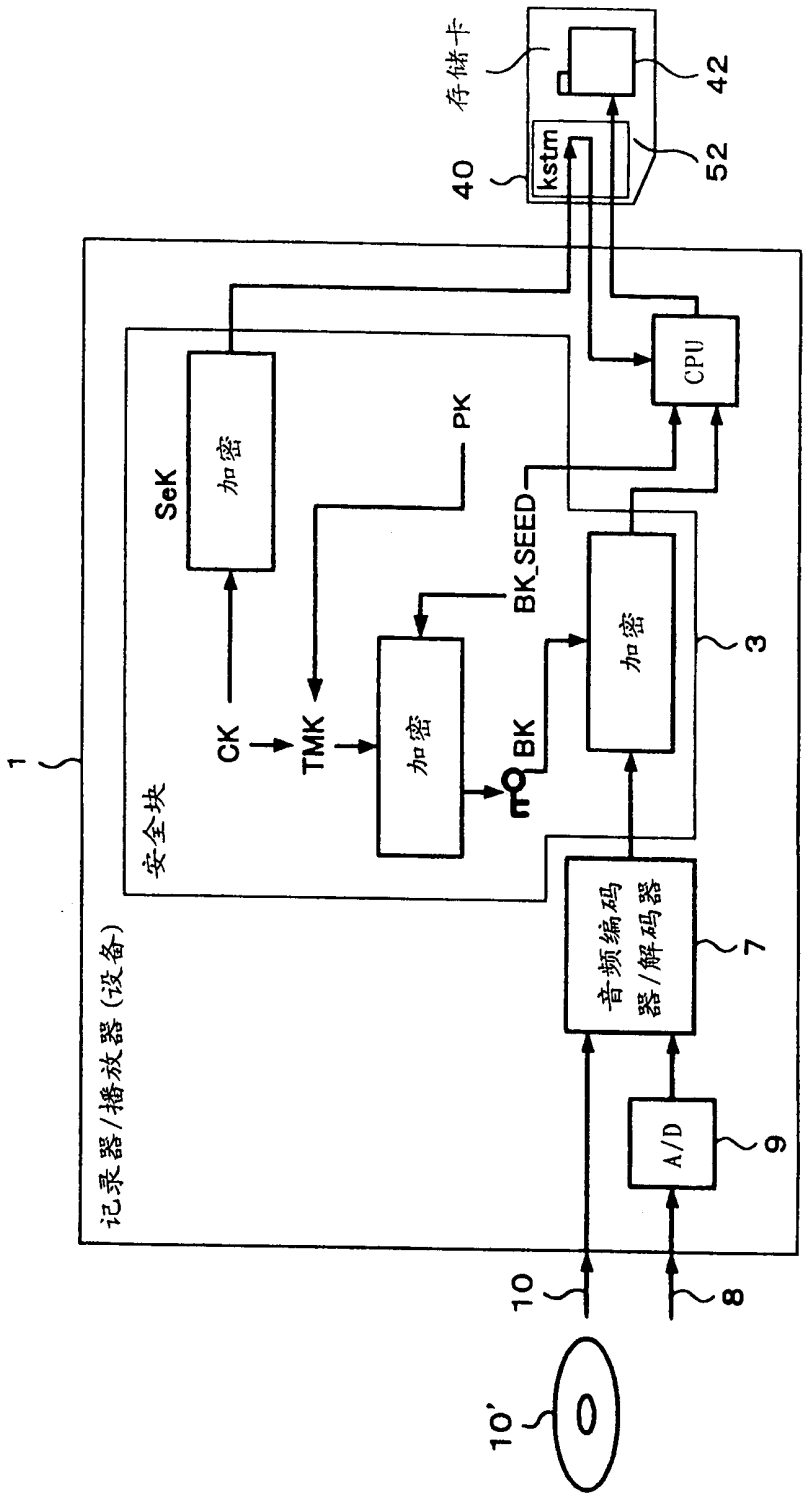

记录器/播放器(设备)
1
安全块
SeK
加密
CK
TMK
加密
BK
PK
BK_SEED
加密
3
CPU
存储卡
40
kstm
52
42
音频编码器/解码器
7
A/D
9
10
8
10'

图 9

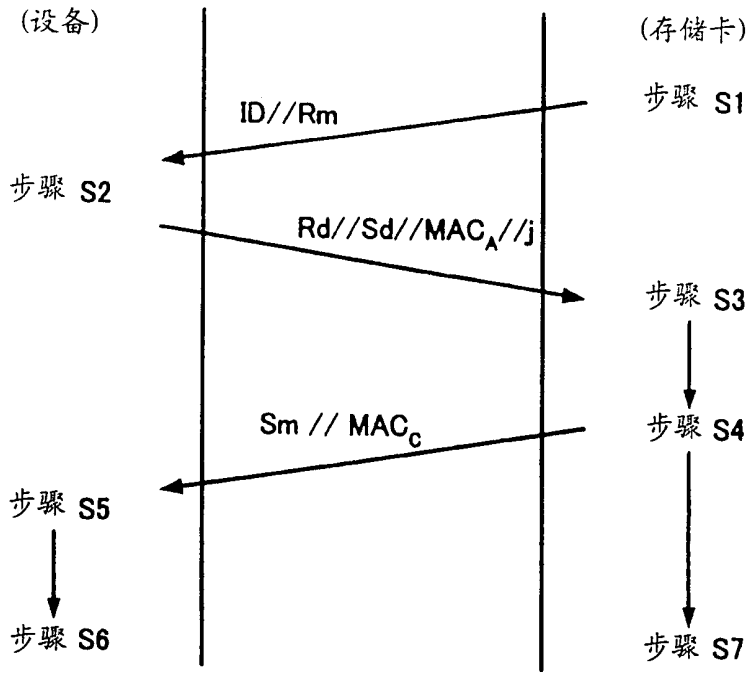

(设备)
(存储卡)
步骤 S1
ID//Rm
步骤 S2
Rd//Sd//MAC$_A$//j
步骤 S3
步骤 S4
Sm // MAC$_C$
步骤 S5
步骤 S6
步骤 S7

图 10

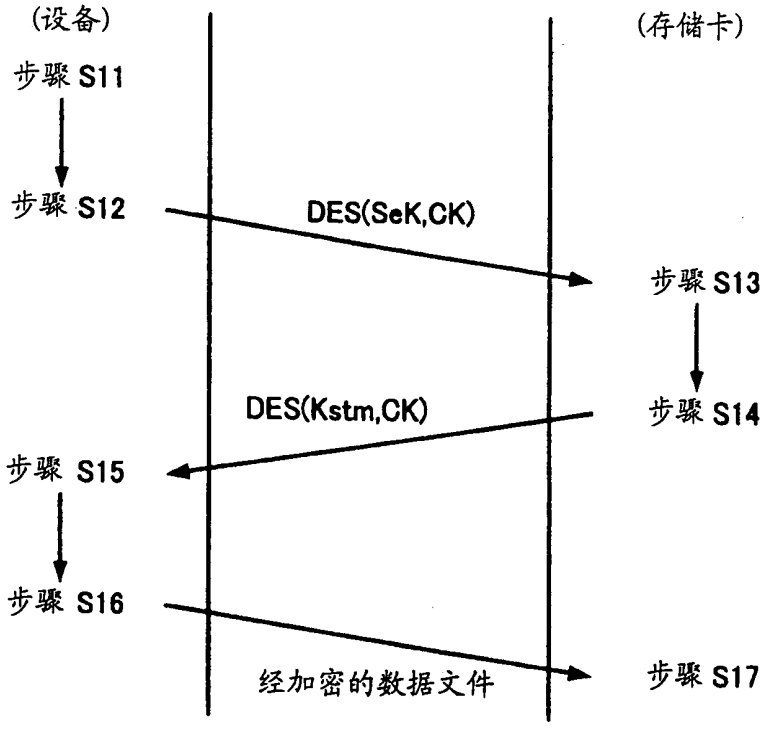

(设备)
(存储卡)
步骤 S11
步骤 S12
DES(SeK,CK)
步骤 S13
步骤 S14
DES(Kstm,CK)
步骤 S15
步骤 S16
经加密的数据文件
步骤 S17

图 11

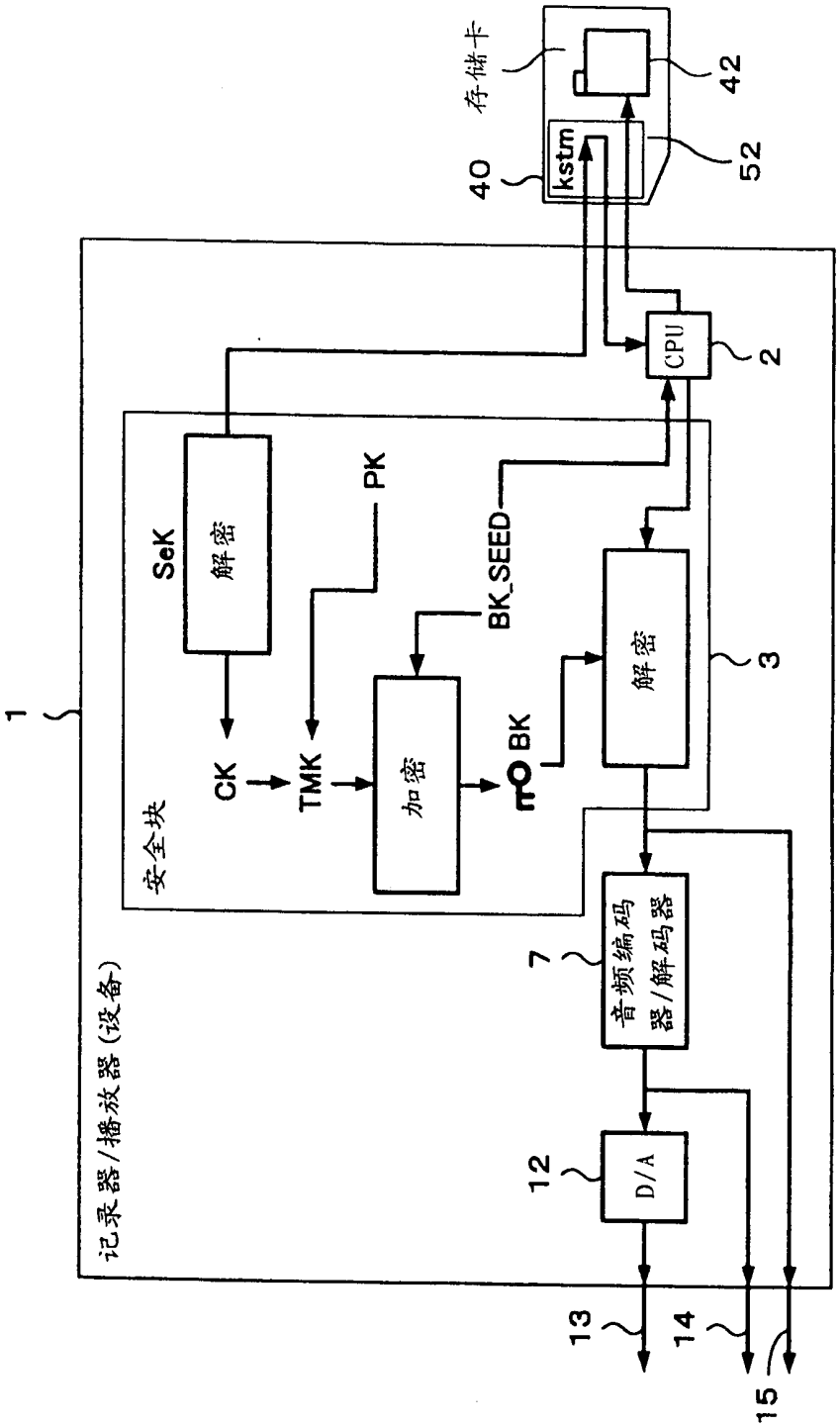

1
记录器/播放器(设备)
安全块
SeK
解密
CK
TMK
加密
PK
BK_SEED
BK
解密
3
CPU
2
存储卡
42
kstm
40
52
7
音频编码器/解码器
12
D/A
13
14
15

图 12

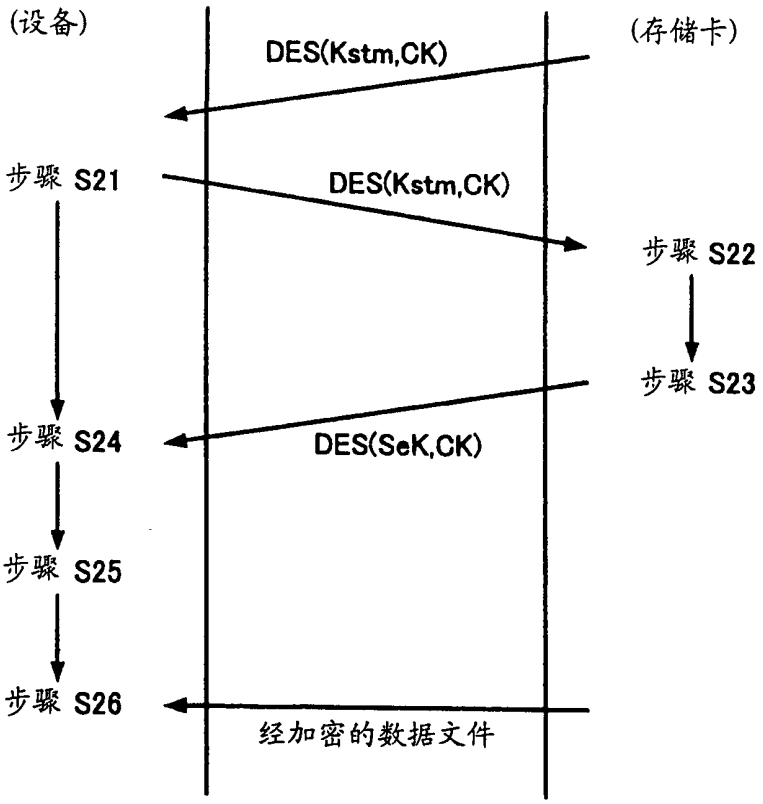

(设备)
(存储卡)
DES(Kstm,CK)
步骤 S21
DES(Kstm,CK)
步骤 S22
步骤 S23
步骤 S24
DES(SeK,CK)
步骤 S25
步骤 S26
经加密的数据文件

图 13

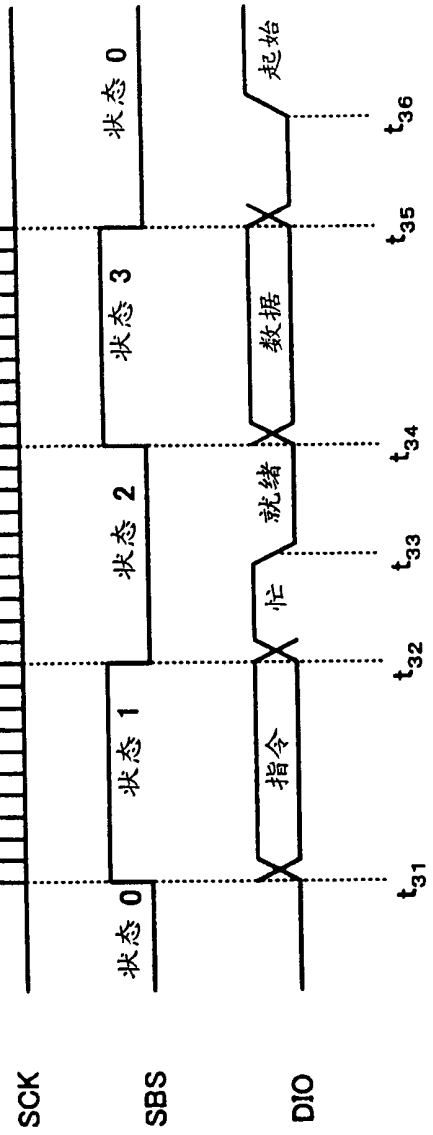

SCK
SBS
DIO
状态 0
状态 1
状态 2
状态 3
状态 0
指令
忙
就绪
数据
起始
t_{31}
t_{32}
t_{33}
t_{34}
t_{35}
t_{36}

图 14

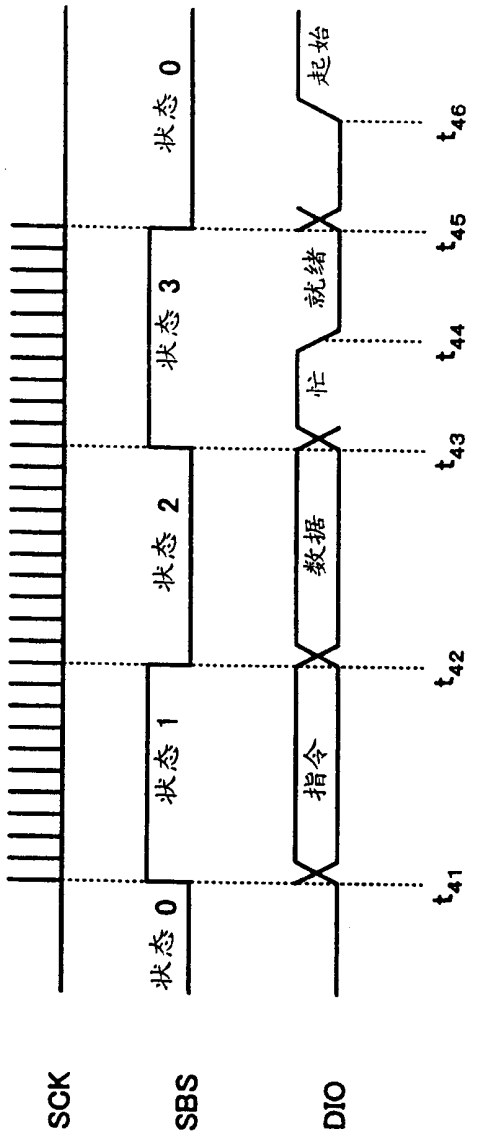

SCK
SBS
DIO
状态 0
状态 1
状态 2
状态 3
状态 0
指令
数据
忙
就绪
起始
t41
t42
t43
t44
t45
t46

图 15

TPC		定义	定义	R/W	数据长度
2Dh	0010 1101	READ_PAGE_DATA →		R	512B+2B(CRC)
D2h	1101 0010	WRITE_PAGE_DATA →		W	512B+2B(CRC)
4Bh	0100 1011	READ_REG →		R	31B+2B(CRC)
B4h	1011 0100	WRITE_REG →		W	15B+2B(CRC)
78h	0111 1000	GET_INT →		R	1B+2B(CRC)
87h	1000 0111	SET_REG_ADRS →		W	4B+2B(CRC)
1Eh	0001 1110	保留	READ_STTS_REG	R	2B+2B(CRC)
E1h	1110 0001	SET-CMD →		W	1B+2B(CRC)
3Ch	0011 1100	保留	READ_SSM_DATA	R	24B+2B(CRC)
C3h	1100 0011	保留	WRITE_SSM_DATA	W	26B+2B(CRC)

图 16

TPC	代码	定义
E1h	AAh	BLOCK_READ
	55h	BLOCK_WRITE
	33h	BLOCK_END
	99h	BLOCK_ERASE
	CCh	STOP
	5Ah	SLEEP
	C3h	CLEAR_BUF
	3Ch	RESET

图 17

TPC	代码	定义	代码	定义
E1h	AAh	BLOCK_READ		
	55h	BLOCK_WRITE		
	33h	BLOCK_END		
	99h	BLOCK_ERASE		
	CCh	STOP		
	5Ah	SLEEP		
	C3h	CLEAR_BUF		
	3Ch	RESET		
	60h	LOAD_ID_CMD	72h	SET_KREC_CMD
	61h	SET_Rm_CMD	73h	MK_KREC_CMD
	62h	MK_Rm_CMD	74h	LOAD_KREC_CMD
	63h	LOAD_Rm_CMD	75h	SET_KPB_CMD
	64h	LOAD_MAC1D_CMD	76h	MK_KPB_CMD
	65h	SET_MAC1M_CMD	77h	LOAD_KPB_CMD
	66h	MK_MAC1M_CMD	78h	CLR_DEC_CMD
	67h	LOAD_MAC1M_CMD	79h	SET_ICV_CMD
	68h	CMP_CMD	7Ah	MK_ICV_CMD
	69h	MK_MAC2M_CMD	7Bh	LOAD_ICV_CMD1
	6Ah	LOAD_MAC2M_CMD	7Ch	LOAD_ICV_CMD2
	6Bh	SET_Sm_CMD	7Dh	LOAD_ICV_CMD3
	6Ch	MK_Sm_CMD	7Eh	LOAD_ICV_CMD4
	6Dh	LOAD_Sm_CMD	7Fh	CMP_ICV_CMD
	6Eh	SET_SeK_CMD	80h	LOAD_NVM_CMD
	6Fh	MK_SeK_CMD	81h	ALLEW_NVM_CMD
	70h	LOAD_SeK_CMD	82h	WR_NVM_CMD
	71h	CLR_IK_CMD	83h	RD_NVM_CMD

图 18

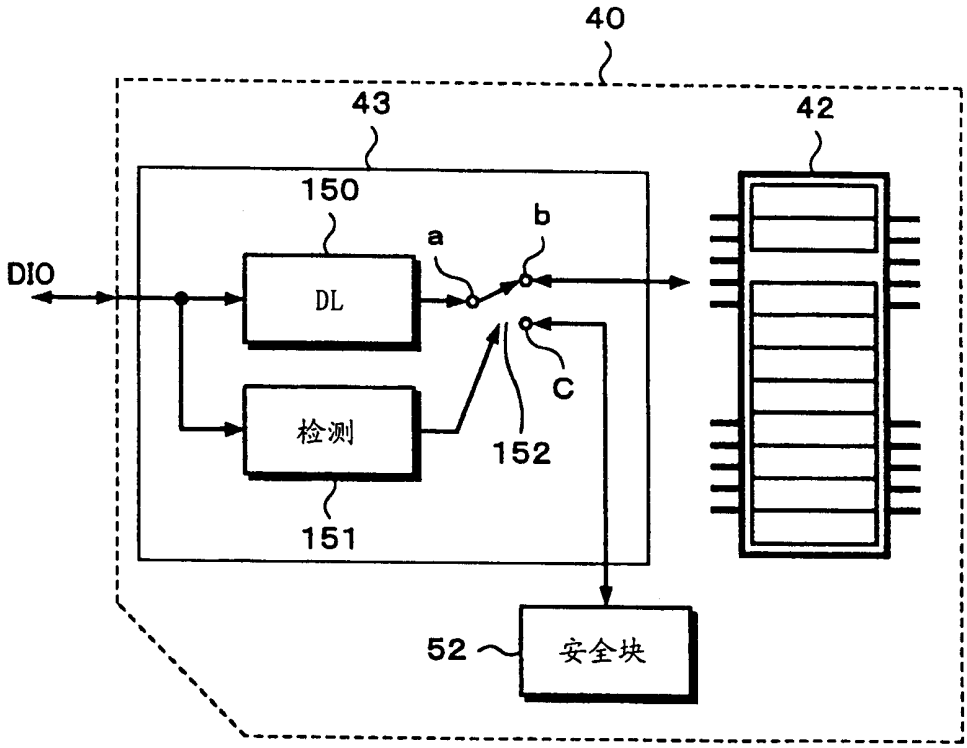


图 19