[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200380104253.3

[43] 公开日 2006 年 1 月 4 日

[11] 公开号 CN 1717639A

[22] 申请日 2003.11.11
[21] 申请号 200380104253.3
[30] 优先权
[32] 2002.11.27 [33] EP [31] 02292935.0
[86] 国际申请 PCT/IB2003/005094 2003.11.11
[87] 国际公布 WO2004/049141 英 2004.6.10
[85] 进入国家阶段日期 2005.5.26
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 E·德斯米奇特 S·穆茨
C·蒂森

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 王 勇

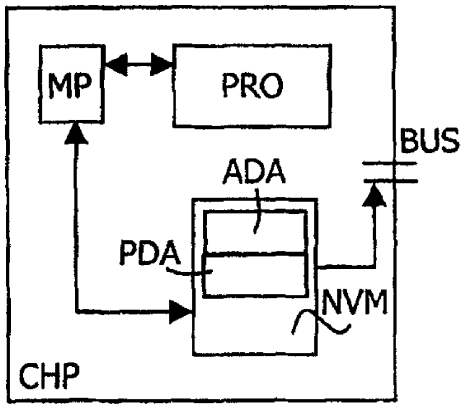
权利要求书 1 页 说明书 16 页 附图 2 页

[54] 发明名称

芯片集成保护装置

[57] 摘要

本发明涉及一种用于处理内容的芯片，至少包括微处理器。 所述芯片包括集成非易失性可编程存储器，用于存储保护数据和受保护数据，所述保护数据目的用于，通过所述微处理器，在执行程序时，批准/否决针对所述受保护数据的访问。 本发明允许保护专门用于芯片集成的有条件访问系统的程序和数据，并允许保护直接位于芯片上的作为外部连接和下载数据的特征。



1. 一种用于处理内容的芯片，至少包括微处理器，其特征在于，所述芯片包括集成的非易失性可编程存储器，用于存储保护数据和受保护数据，所述保护数据目的用于在执行程序时，通过所述微处理器批准/否决对所述受保护数据的访问。

2. 权利要求 1 的芯片，其中所述保护数据仅能可以修改以增强该保护。

3. 权利要求 1 或 2 中一个的芯片，其中所述保护数据包括密码，所述访问通过密码检查而被批准/否决。

4. 权利要求 1 至 3 中一个的芯片，其中所述受保护数据包括用于激活/停止芯片的任选特征的数据。

5. 权利要求 4 的芯片，其中所述任选特征是到外部设备的连接，用于从所述外部设备下载程序和/或数据。

6. 权利要求 4 的芯片，其中所述受保护数据包括用于激活/停止用于所述微处理器的外部引导程序的数据，所述外部引导程序包括用于从外部存储器下载用于所述微处理器的新引导程序的指令。

7. 权利要求 1 或 2 中一个的芯片，其中所述保护数据包括定义了地址限制的值，从该地址限制起，存储在所述存储器的数据是受保护数据，并且对该受保护数据的访问被否决。

8. 权利要求 7 的芯片，其中所述受保护数据包括用于操作有条件访问专用微处理器的程序和数据。

9. 一种用于从介质中恢复内容并处理所述内容的设备，所述设备包括到所述介质和如权利要求 1 至 8 所述芯片的连接。

10. 权利要求 10 的设备，用于处理加密视频/音频数据。

11. 一种用于获得至少包括微处理器的受保护芯片的方法，所述方法使用如权利要求 1 至 8 中一个所述的芯片，所述方法包括步骤：

- 至少使用已批准的访问，用以修改所述非易失性存储器中的受保护数据，

- 通过修改保护数据以便于否决访问，来保护对非易失性存储器中的所述受保护数据的访问。

芯片集成保护装置

技术领域

本发明涉及一种用于处理内容的芯片，至少包括微处理器。本发明特别涉及意图要嵌入在设计用于从介质中恢复受保护内容的设备中的芯片。本发明还涉及其中嵌入了该芯片的设备。本发明还涉及一种保护根据本发明的该芯片的方法。

背景技术

在已知的专门用于内容处理的设备中，需要受保护的所述内容、所述内容的安全通常是由处理内容的芯片（在下文中被称为主芯片）外部的装置进行控制的。该外部安全装置包括智能卡系统，例如，如文献 EP11050506 中所描述的。该外部安全装置的优点在于它们提供了设备保护的良好的灵活性。

然而，在该文献中，包括内容处理装置的芯片，以及由此所致的系统内核，不是由其自身保护的。目的用于连接外部元件的连接器，例如，用于测试芯片的总线，可用于获得对内容处理装置的控制。这样，经处理的内容是可访问的，且不再受到保护。而且，主芯片和安全元件之间的隔离意味着此两者之间的通信可能遭到窃听。而且，现有技术领域中提出的安全装置是昂贵的，并且需要增补的制造步骤以在设备中进行实现。

发明内容

本发明的目的在于解决所有上文提及的缺陷。本发明的另一目的在于提出低价的安全设备。

通过如权利要求 1～8 中的一个所要求的芯片和如权利要求 9 或 10 中所要求的设备，实现了此目的。根据本发明的芯片包括集成非易失性可编程存储器，用于存储保护数据和受保护数据，所述保护数据目的用于，通过所述微处理器，在执行程序时，批准/否决针对所述受保护数据的访问。

在包括处理装置的芯片中插入此非易失性可编程存储器，允许为

所述芯片的不同特征提供集成保护。所述微处理器进行的访问可以具有写或者读的方式。本发明使得灵活的安全装置能够以非常简单和低成本的直接方式实现在主芯片中。在第一实施例中，受保护的数据定义了所述芯片的特征，并且所述微处理器被批准或者未被批准以写或者读的方式访问所述受保护数据。例如，该特征可以是针对外部元件的连接，例如，如用于测试芯片的总线。这样，本发明允许避免该连接获得对微处理器的控制。需要访问受保护数据的微处理器具有一种程序，使其检查保护数据批准还是否决所述访问。如果在所述芯片中存在数个微处理器，则每个微处理器具有其自己的保护数据用于其自己的针对受保护数据的访问。当保护可以提供不同种类的保护且受保护数据可以对应于关于所述芯片的数种特征时，本发明允许多种保护。在下文中，根据本发明的原理提出了数个实施例。

有利地，保护数据仅为可修改的增加保护。因此，当保护数据已被修改以便于否决访问时，不再可能访问受保护数据。

根据本发明的第一实施例，可由所述保护数据采用的每个值具有关于所述微处理器的程序的具体意义：针对给定受保护数据的访问被批准，或者否决，或者有条件地批准。因此，有利的实现方案提出了，保护数据包括密码，所述访问通过密码检查而被批准/否决。

第一实施例可用于包括用于激活/停止芯片任选特征的数据的受保护数据。该任选特征可以是目的在于连接到外部设备用于自所述外部设备下载程序和/或数据的连接。该任选特征可以是用于所述微处理器的外部引导程序，所述外部引导程序包括用于自外部存储器下载关于所述微处理器的新的引导程序的指令。该任选特征可以是任何能够在芯片中有利地被激活/停止的特征。因此，该第一实施例使得能够定制芯片的特征。

根据本发明的第二实施例，保护数据包括定义地址限制的值，在所述非易失性存储器的该地址限制下，所存储的数据是受保护数据，并且针对该受保护数据的访问被否决。在该实施例中，保护数据构成了关于所述微处理器的程序的限制，在该限制下访问被否决。有利地，保护仅可以被增强，并且所述值仅可被修改用于增强。

在该第二实施例的应用中，受保护数据包括专门用于有条件访问专用微处理器的机能的程序和数据。所述有条件访问专用微处理器目

的在于，如现有技术领域所知的，与所述芯片处理的内容中存在的安全数据进行交互。因此，根据本发明的原理，通过允许在主芯片中由其自身保护程序和数据，允许在主芯片中实现安全装置。该安全装置可以与出现在智能卡芯片上的安全装置相似。

根据此第二有利实施例，还可以保护任何下载的数种程序和数据：引导程序、有条件访问程序....。

这样，本发明使得该芯片能够得到保护，在所述微处理器和存在于芯片上的安全元件之间进行通信时黑客将不能监听，这是因为这些安全元件将在芯片自身中实现。

本发明还涉及目的在于从介质中恢复内容并处理所述内容的设备，所述设备包括针对所述介质的连接以及如上文所述的芯片。有利地，所述设备目的在于处理加密视频/音频数据。

本发明还涉及用于获得至少包括微处理器的受保护芯片的方法，所述方法使用至少包括集成非易失性可编程存储器的芯片，其被称为非易失性存储器，所述非易失性存储器包括保护数据，所述保护数据目的用于，通过所述微处理器，在执行程序时，批准/否决针对所述非易失性存储器中的受保护数据的访问，所述方法包括步骤：

至少使用批准的访问以修改所述非易失性存储器中的受保护数据，

通过修改保护数据以便于否决所述访问，保护针对所述非易失性存储器中的所述受保护数据的访问。

附图说明

下文通过参考附图详细描述了本发明，其中：

图 1a 和 1b 说明了根据现有技术的设备；

图 2 说明了根据本发明的芯片；

图 3 说明了根据本发明的示意性的可编程非易失性存储器；

图 4 说明了根据本发明的优选实施例的芯片。

具体实施方式

图 1 示出了根据现有技术的设备 DEV。这种设备 DEV 意图用于从介质 VCM 中恢复内容。所述内容可以是接收的信号，来自磁盘的数

据...。所述介质可以是网络（卫星、地面、电缆、无线...）、DVD、闪存卡、个人录影机的硬盘...。所述设备可以是机顶盒、TV 接收机、DVD 播放机、连接的家庭服务器、便携式音频播放机、移动电话...。

所述设备 DEV 至少包括芯片 CHP，其至少包括具有程序 PRO 的微处理器 MP，用于处理从所述介质 VCM 中恢复的内容。通常，经处理的内容然后传输到宣传装置 EXP。这些宣传装置 EXP 例如能够将经处理的数据显示为图像。所述宣传装置 EXP 可以包含在所述设备中，或者在所述设备外部，其不会造成任何差别。

在现有技术中，所述设备 DEV 通常包括安全专用部分，其是作为与所述芯片 CHP 分离的有条件访问系统而实现的。在图 1 呈现的示例中，该有条件访问系统由智能卡读卡器 SCR 表示，其能够在微处理器 CMP 的协助下读取智能卡 SC。

图 1b 示出了根据现有技术的另一实现方案：可移动安全模块 SCR 作为安全专用部分插入到设备中。其从介质 VCM 中接收加扰内容，对它们进行解密，并且然后将它们发送到内容处理装置。在现有技术中，将包括处理装置的主芯片 CHP 出售为实现在所述设备 DEV 中，而没有任何集成的保护。在此一般性的情况中，由安全专用部分接收和控制的数据需要发送到未受保护的主芯片。这种通信可以通过例如用于测试芯片 CHP 的总线来监听。而且，这种总线可以控制在所述主芯片 CHP 上实现的任何微处理器。这样，不再能够确保系统的安全。当需要受保护的内容在芯片 CHP 中进行处理时，这是一个极其重要的问题。本发明的目的在于使这种芯片 CHP 能够具有集成保护。根据图 2，本发明提出了芯片 CHP 至少包括集成非易失性可编程存储器，称为非易失性存储器 NVM，所述非易失性存储器 NVM 包括保护数据 ADA 和受保护数据 PDA，所述保护数据目的用于通过所述微处理器 MP，在程序 PRO 的执行之下，批准/否决针对所述受保护数据 PDA 的访问。

图 3 说明了根据本发明的非易失性存储器的内容原理。

所述可编程非易失性存储器可以是快闪存储器、可编程只读存储器（PROM）、非易失性随机访问存储器（NVRAM）、磁随机访问存储器（MRAM）、一次性可编程存储器...。图 3 中示出的非易失性存储器可以是独立的可编程非易失性存储器，或者是分区可编程非易失性存储器的一部分。如图 3 呈现的单一的存储器可以实现根据本发明的数

个实施例并在下文呈现，或者可以专用于实现单一的实施例。

根据本发明的原理，保护数据 ADA 存储在非易失性存储器 NVM 的第一地址 AD1。所述保护数据 ADA 保护针对所述非易失性存储器 NVM 中包括受保护数据 PDA 的地址 AD2 的访问。所述访问可能是读或者写或者读和写两者，如下文中将示出的。

在下面的图和表中提出了根据本发明的使用保护数据和受保护数据的数个实施例。所给出的这些实施例能够使本领域的技术人员理解、再现和使用本发明，在不偏离本发明的范围前提下，还可以修改位于不同地址的其他种类的保护数据和受保护数据。

保护数据 ADA 的示例：

在第一实施例中，可由所述保护数据 PDA 采用的每个值具有对于所述微处理器 MP 的程序 PRO 的特定意义：针对存储在一个地址或者数个地址 AD2 的给定的受保护数据 PDA 的访问，由所述程序 PRO 已知的，被批准或者否决、或者有条件地批准。

在根据该第一实施例的保护数据的第一简单实现方案中，存储在地址 AD1 中的保护数据可以采用两个值：0 和 1。例如，0 对应于被批准的访问而 1 对应于未批准的访问。

地址 AD1	值	保护数据的名称
1 位:	0/1	ACCESS_CONTROL

因此，如果值是 0，则针对地址 AD2 的访问是可利用的。在该情况中，如果值是 1，则访问被拒绝。这样，地址 AD2 是受到保护的。有利地，可以仅增加该保护。在该示例中，这意味着 ACCESS_CONTROL 位仅可被设为从 0 到 1。当然，根据本发明，同样可行的是对于被设为 1 的位允许对地址 AD2 的访问，并且对于被设为 0 的位禁止这种访问。每次访问被定义为写、读、或者写和读两者，并且相对于一个或者数个给定的地址 AD2 进行定义。地址 AD2 中的受保护数据 PDA（数据、程序、选项...）的数个示例将在下文中给出。

保护数据 PDA 的有利的实现方案使用密码检查。其允许中间制造商（如最终设备制造商或者广播运营商）使用密码来保持对某些具有防止盗版的第一保护级别的数据和/或程序或者选项进行访问的可能

性。在该情况中，保护数据以两位进行编码。

下面的表中给出了该实现方案的示例：

地址 AD1	值	保护数据的名称
2 位：	0: 0/0: 1/1: X	ACCESS_CONTROL
Y 位：		SAVED_PASSWORD

在该具有密码控制的实施例中，ACCESS_CONTROL 位被用于定义保护级别：被批准访问或者不被批准访问。

如果值=0: 0，则批准针对存储在地址 AD2 的数据的访问，所述地址 AD2 和所述非易失性存储器以及因此的所述芯片未受保护。有可能读并且写 SAVED_PASSWORD 的 Y 个位。

如果值=0: 1，则非易失性存储器和芯片由密码保护。不再可能读或者写 Y 个位的 SAVED_PASSWORD。为了实现密码控制，非易失性存储器例如连接到 Y 个位的寄存器。在该寄存器中可以写 Y 个位的 ENTERED_PASSWORD 的密码。然后该密码同保存在非易失性存储器中地址 AD1 的名称为 SAVED_PASSWORD 的密码进行比较。该比较可以使用由简单的反相器、与门和或门构成的简单的随机逻辑。

两种情况是可能的：

写在寄存器中的密码是正确的，这意味着 ENTERED_PASSWORD 和 SAVED_PASSWORD 是相同的。针对地址 AD2 中存储的数据的访问得到批准，这意味着非易失性存储器处于未受保护模式。

写在寄存器中的密码不是正确的。针对地址 AD2 中存储的数据的访问未得到批准，这意味着非易失性存储器处于受保护模式。

只要非易失性存储器处于未受保护模式，即可以读或者写所述地址 SAVED_PASSWORD，一旦当芯片由密码或者硬件保护时，既不能读也不能写所述地址 SAVED_PASSWORD。

如果值=1: X，X 是 0 或者 1，则针对地址 AD2 的访问由硬件保护。

此外，可以仅提高保护级别，其从不降低。这样，从 1: X 到 0: X 或者从 0: 1 到 0: 0 是不可能的。这种特征是使用单向状态机实现的。状态机有效地定义了不同的状态，可以以给定的和固定的顺序采用这些状态。可以对状态进行排序以实现循环：一旦到达了状态列表的最

后状态，则该列表的第一个状态是下一个状态，或者状态可以以开路的方式进行排序。在该情况中，获得了单向状态机，由于其仅允许遵守状态中的给定顺序，并且一旦到达了最后状态，不再有可能改变状态。

在第二实施例中，存储在地址 AD1 的保护数据 ADA 定义了地址限制，在该限制下，针对所述非易失性存储器 NVM 的访问被禁止，所述保护数据仅可以被修改为仅使之增加。再次说明，对于给定的微处理器，所述访问可以再次被定义为写或者读、或者写和读两者。

例如，非易失性存储器 NVM 的最后填充的地址 AD1 包含名称为 READ_AND_WRITE_LIMIT 的值作为保护数据 ADA。微处理器 MP 既不能读也不能写小于该值 READ_AND_WRITE_LIMIT 的所有地址 AD2。由存储在小于该值 READ_AND_WRITE_LIMIT 的地址的任意数据来定义受保护数据 PDA。所有大于该值的地址可以由所述微处理器读或者写。可以读存储在 AD1 的值。而且，只有当新的值大于旧的值时，其才能够被写入。而且，由于地址限制 READ_AND_WRITE_LIMIT 仅可以被增加，所以保护仅可以被增加。

在另一示例中，非易失性存储器 NVM 的最后地址 AD1 包含读限制 READ_LIMIT 和/或写限制 WRITE_LIMIT。所有小于 READ_LIMIT 的地址均不能由所述微处理器读取。所有等于或者大于该值的地址均可由所述微处理器读取。所有小于 WRITE_LIMIT 的地址均不能由所述微处理器写入。所有等于或者大于该值的地址均可由所述微处理器写入。

只有新的值大于旧的值时，微处理器才能够读取并修改 READ_LIMIT 和 WRITE_LIMIT。因此，保护级别仅可以被增加，并且非易失性存储器 NVM 的受保护部分不断变得更大。在该第二实施例中，用于控制访问的地址是小于存储在 AD1 的值的地址 AD2。

非易失性存储器中的受保护数据 PDA 的示例:

如上文所见，对于给定的微处理器，地址 AD1 的保护数据目的在于保护对非易失性可编程存储器 NVM 的其他地址 AD2 的用于写和/或用于读的访问。受保护数据 PDA 存储在所述地址 AD2。下面将给出可以存储在受保护地址 AD2 的受保护数据 PDA 的示例。

第一种受保护数据 PDA 可以是定义了芯片 CHP 的特征状态的特征数据。这里，由存储在地址 AD1 的所述保护数据 ADA 控制的访问通常

是由微处理器在地址 AD2 进行的读访问。微处理器可以读特征数据，但是由保护数据 ADA 来决定是否批准其写访问。

该特征可以是在所述芯片 CHP 上实现的选项，并且因此特征数据给出或者不给出使用该选项的批准。该选项的示例是那些通常在许可支付条件下实现的选项。例如，SECAM、MACROVISION、ICAM、CCIR_OUTPUT 是此类选项。这样，可以在制造过程中在所有芯片中实现用于实现这些选项的装置，并且随后通过实现如本发明所提出的由保护数据 ADA 控制的保护级别，可以启用或禁用它们的使用。在所有芯片中用于实现这些选项的所有装置的实现方案、以及根据最终设备制造商或者广播运营商的选择的最终定制，允许实现关于所述芯片研发和制造的成本节约。实际上，可以制备单一形式的该芯片。该芯片在最终的生产阶段进行定制。其灵活性是原始的。在下表中给出了存储受保护数据 PDA 的四个地址 AD2，用于通过使用第二列中的值选择第三列中命名的选项。

地址 AD2	值	特征的名称
1 位:	0/1	ENABLE_SECAM
1 位:	0/1	ENABLE_MACROVISION
1 位:	0/1	ENABLE_ICAM
1 位:	0/1	ENABLE_CCIR_OUTPUT

根据对于四个地址 AD2 每一个的该位的值，可以使 CCIR_OUTPUT 特征是可获得的或者是不可获得的，可以启用或不启用 ICAM 特征，在芯片 CHP 上实现的处理装置可以向处理装置的输出添加或者不添加 MACROVISION 复制保护，在芯片 CHP 上实现的处理装置可以产生或者不产生 SECAM 输出。这样，通过存储在地址 AD1 的对应的保护数据 ADA，批准或者不批准用于改变这些值的访问。

然后，如本发明的所述第一实施例中所给出的，在保护数据 ADA 的控制下，提供选项的控制。优选地，存储在地址 AD1 的保护数据 ADA 的单一位保护选项组。然而，存储在地址 AD1 的数个保护数据 ADA 还可以单独地保护每个上述的地址 AD2。

由保护数据 ADA 保护的特征可以是允许芯片 CHP 的外部连接的任

何装置。本发明允许通过控制其状态：有效或无效的特征数据，使这种装置启用或者禁用。该装置在下文中给出。

微处理器的引导模式：

由于本发明，微处理器可以具有被称为第一引导模式的小程序，其存储在芯片上的任何存储器的一小部分中，用于实现其来自外部存储器的第一引导。例如，芯片外部和/或最终设备外部（如果芯片已用于该设备）的 EEPROM 可以用作外部存储器。这样，广播运营商可以从此外部存储器下载新的引导程序，该引导程序可以随意定制。由微处理器通过读其中存储了特征数据的地址 AD2，执行所述内部或者外部第一引导模式的内部或者外部的激活（参看下文的示例和表格）。事实上，本发明通过修改存储在地址 AD2 的定义了引导模式（内部或者外部）的受保护数据 PDA，允许禁用或者启用第一引导模式的激活，用以下载引导程序。然后，存储在地址 AD1 中的如本发明第一实施例中定义的保护数据 ADA 控制对定义了引导模式的受保护特征数据 ADA 的写访问。一旦通过将地址 AD2 从“外部引导”改变为“内部引导”来使该第一引导模式的这种激活禁用，以及一旦根据一个所述实施例，通过地址 AD1 的保护数据 ADA 而未批准地址 AD2 的写访问，用于地址 AD2 的写访问不再是可能的，并且“外部”引导模式不再是可能的。这样，引导从芯片中已存储了新的引导程序的存储器中实现。

允许对芯片内部访问的连接：

根据本发明，可以使所述芯片到外部源的连接禁用。JTAG、EJTAG、调试接口可以允许外部用户控制或者监听芯片的内部操作，并且本发明特别关注该特征。该特征的状态（激活或者不激活）由存储在地址 AD2 的受保护数据 PDA（参看下面的表格）定义。根据本发明的第一实施例，由保护数据 ADA 控制用于该地址 AD2 的写访问。

这是关于现有技术的新的功能，其中主要用于制造或者调试用途的这些连接通常由于安全上的原因而受到物理上的抑制，带来了特别涉及芯片测试的固有缺陷。本发明允许保留此用于测试芯片和/或设备的连接，并且然后通过不可逆的方式使之禁用。在最终设备商品化之前，可以通过简单的编程实现该禁用。

批准写入程序和数据用于微处理器的操作：

通过在地址 AD2 存储 READ_ONLY 值作为受保护数据 PDA，在该值下地址不能被写入，也可以禁止写所述非易失性存储器 NVM 的地址。只要相对应的保护数据 ADA 允许访问修改所述受保护数据 PDA，则可以修改所述值 READ_ONLY。

根据第二实施例的保护数据 ADA 可以用于保护第二类受保护数据 PDA，其包括存储在芯片中的程序和数据。例如，在下载用于微处理器的程序和数据之后，本发明进一步允许控制针对所述下载程序和数据的访问。这对于其中专门用于有条件访问系统的程序和数据是在芯片自身中下载的所述芯片是特别有利的。事实上，由于本发明，安全的有条件访问单元可以集成到芯片自身。事实上，根据如图 4 呈现的本发明的优选实施例，可以使有条件访问单元 CAS 位于芯片 CHP 自身中。事实上，本发明允许具有保护，以便于避免读取专门用于有条件访问单元 CAS 的安全操作的程序和数据。如果希望在芯片中使用有条件访问单元 CAS，则该特征是重要的。

通常，有条件访问单元 CAS 包括专用微处理器 CMP。事实上，主微处理器具有大的程序和数据，其不能有效地得到保护。通常，这是专门指定另一微处理器用于该功能的原因。常用于智能卡系统的该微处理器的示例具有 Intel 80c51 指令集。根据本发明，此类微处理器有利地在芯片上实现。为了对该微处理器 CMP 进行编程，根据本发明，广播运营商不受限制地选择其需要的任何程序：用于对管理消息（例如 ECM 和 EMM 消息）进行解密的算法、加密算法，并且不受限制地选择其需要的用于在有条件访问单元 CAS 中实现的安全特征。只要下载装置由如上文给出的特征数据激活，则可以下载常用的用于解密 ECM 消息的 Triple-Des 算法、常用的 RSA 算法或者具有公-私钥系统的椭圆曲线…。这样，根据所下载的程序，可以管理高级特征，诸如按次计费（pay-per-view）、家长控制…。本发明的一个优点在于给出了这些可能选择而不失安全性，这是因为，一旦存储了所述算法，则根据本发明的第二实施例，通过在地址 AD1 至少存储限制值，在该值下读和/或写是被禁止的，保护数据 ADA 提供了不批准具有针对所述程序和数据的读和/或写访问的可能性。这里，访问的控制涉及主微处理器的访问，而不涉及有条件访问微处理器的访问，其不得不进行某些针对其中存储了有条件访问程序和数据的非易失性存储器的

读和写访问。事实上，在最低地址存储了一个或者多个密钥，并且在上面的地址存储了访问权限。访问权限给出了数据，用以了解有条件访问微处理器将接受哪些程序以提供解码密钥，并且主微处理器需要这些数据，因此其具有读它们的权限。这样，由于根据本发明的第二有利实施例的保护数据 ADA 的实现方案，主微处理器既不能读也不能写最低地址，并且可以读但是不能写存储访问权限的上面的地址。

有利地，使用另外的内部 SRAM 存储器存储算法运算过程中的中间结果。通过进行构建，此最终的 SRAM 存储器不能由主微控制器读或者写，这意味着不存在该存储器和主微处理器之间的连接：该 SRAM 仅具有同有条件访问微处理器的连接。

可以同其他根据本发明的实施例组合或并置使用的优选实施例对于机顶盒设备而言是特别便利的，其有利地具有有条件访问系统。

下面给出了在机顶盒设备的情况中的所示不同实施例的组合的示例。在该示例中，如图 4 中所述，主芯片 CHP 至少包括微处理器 MP 和可以分区的快闪存储器 NVMS。所述微处理器 MP 是，例如，具有 MIPS 指令集的处理器。有利地，所述快闪存储器 NVMS 未直接连接到微处理器-总线，而是在微处理器-总线和快闪存储器之间插入了简单的随机逻辑，以便于有力地封闭环境。

在快闪存储器 NVMS 的上面地址存储了保护数据 ADA，其可以分为三个组：Access_Control_Group（访问控制组）、MIPS_Protection_Group(MIPS 保护组)和 Selection_Options_Group（选择选项组）。

Access_Control_Group 由下表中给出的地址 AD1 构成。

地址 AD1	值	保护数据的名称
1 位：	0/1	Selection_Options_ACCESS_CONTROL
2 位：	0:0/0:1/1:X	MIPS_Protection_ACCESS_CONTROL
Y 位：		SAVED_PASSWORD

X 是 0 或 1，并且 Y 是密码 SAVED_PASSWORD 加扰的位数目。

根据上面的实施例，保护数据是否对应于

MIPS_Protection_ACCESS_CONTROL 允许主微处理器写访问 MIPS_Protection_Group 。在下表中定义了所述 MIPS_Protection_Group 的受保护数据:

地址 AD2	值	保护数据/特征的名称
1 位:	0/1	BOOT_MODE
2 位:	0/1	DISABLE_BUS
Z 位:		READ_ONLY

上文已经给出了附于这些受保护数据的特征。例如，BOOT_MODE (引导模式)的值为 0,则可以使用来自外部存储器的引导,BOOT_MODE 的值为 1，则由内部非易失性存储器实现引导，例如，其来自其中存储了下载引导程序的本发明的集成非易失性存储器。

有利地，包括所述微处理器程序的非易失性存储器可以直接连接到微处理器，或者可以在微处理器连接总线和非易失性存储器之间插入简单的随机逻辑（也被称为胶联逻辑），以便于保护连接。

例如，DISABLE_BUS 的值为 0，则相关的连接总线可以用作用于测试芯片或者最终设备并用于随意装载任何所需程序和数据的连接装置。如果 DISABLE_BUS 的值为 1，则不能再使用所述连接总线。这样，通过根据本发明的第一实施例改变所使用的相关的保护数据 ADA，使得受保护数据 DISABLE_BUS 的值不再是可访问的。这样，根据本发明，以这样的方式可以保护任何下载和/或连接装置。

仅在非易失性存储器根据存储在地址 AD1 中的值处于未受保护模式时，也即意味着，非易失性存储器是未受保护的 (MIPS_Protection_ACCESS_CONTROL=0:0)或者通过输入的有效密码由密码保护非易失性存储器 (MIPS_Protection_ACCESS_CONTROL=0:1)时，上面的受保护数据才能够改变。

保护数据是否对应于 Selection_Option_ACCESS_CONTROL 允许主微处理器写访问 Selection_Options_Group。在下表中定义了所述 Selection_Options_Group 的受保护数据:

地址 AD2	值	保护数据/特征的名称
1 位:	0/1	ENABLE_SECAM
1 位:	0/1	ENABLE_MACROVISION
1 位:	0/1	ENABLE_ICAM
1 位:	0/1	ENABLE_CCIR_OUTPUT

例如，这里非易失性存储器的保护（由 MIPS_Protection_ACCESS_CONTROL 定义）被选择为对该组没有影响。仅考虑 Selection_Options_ACCESS_CONTROL 的值。

该示例的芯片还包括可编程非易失性存储器 NVMC，或者在芯片上实现专门用于有条件访问单元的一部分可编程非易失性存储器 NVMC。所述非易失性存储器 NVMC 包括两个部分 NVMC1 和 NVMC2，其中分别存储用于有条件访问微处理器 CMP 的机能的程序和数据。所述部分 NVMC1 和 NVMC2 在它们的最高地址中包括根据本发明的第二实施例的保护数据 ADA。

根据本发明，本发明还涉及定制和保护芯片的方法。所述方法使用至少包括集成非易失性可编程存储器的芯片，所述非易失性存储器包括保护数据，所述保护数据至少定义了关于针对所述非易失性存储器的访问的保护级别，所述保护数据仅可被编程用于增加保护级别。

第一步骤是，至少使用未受保护的访问以修改所述非易失性存储器中的数据，第二步骤是，通过修改保护数据，增加关于所述访问的保护级别，由此保护针对非易失性存储器中的所述数据的访问。由于根据本发明可以保护重要的特征，因此由本发明的方法获得了受保护的芯片。该受保护芯片有利地趋于在专门用于连接介质的设备中实现，其至少包括用于处理恢复从所述介质中的数据的微处理器。例如，所述微处理器控制用于处理音频/视频数据的加扰/解码装置。

事实上，根据本发明，保护数据的值可以改变，因此保护可以在最终的受保护芯片的制造过程中得到增强。下面给出了定制芯片的方法的示例。所述保护数据可以实现在相同芯片中的一个或者数个可编程非易失性存储器中。

然后，给出了上文提出的芯片示例中描述的开发芯片，以便于获得全面受保护的芯片的方法。然后，下面给出了在不同的环境中使用

该方法的两个步骤的事件链的示例。希望制造定制的和安全的最终设备的广播运营商有利地使用在芯片自身上的或者甚至在所述最终设备中实现的芯片上的所述事件链。根据本发明，最终设备制造商和广播运营商仅需要对芯片进行编程以实现获得受保护芯片的方法的装置。

未受保护的芯片递送到最终设备制造商或者广播运营商，其具有来自外部存储器的缺省引导模式（BOOT_MODE=0）。任何将变为集成在芯片上的本发明的非易失性存储器的存储器仍未受到保护，并且对其的访问得到批准。这样，最终设备制造商或者广播运营商必须执行下面的软件处理：

－对有条件访问单元 CAS 的非易失性存储器 NVMC 的部分 NVMC1 中的有条件访问微处理器 CMP 的程序 PRG 进行编程。在该程序中包括了用于获得定制的和完整的有条件访问系统的所有软件。例如，广播运营商不受限制地选择将用于此目的的加密算法（RSA 等）。

－通过对保护数据 ADA 编程，其是非易失性存储器的所述部分 NVMC1 的部分 NVMC1 的最高地址处的值，用以禁止主微处理器读或者写该程序的最低地址，保护此有条件访问微处理器 CMP 的程序。根据第二实施例实现包括有条件访问程序的非易失性存储器 NVMC 的此保护。这样，所述部分 NVMC1 是根据图 3 所说明的本发明的原理的非易失性存储器 NVM。

－对有条件访问单元 CAS 的非易失性存储器 NVMC 的部分 NVMC2 中的有条件访问微处理器 CMP 的数据 DAT 进行编程。解密密钥（RSA 等）引入到分配给这些数据的最低地址。

－通过在所述部分 NVMC2 的最高地址存储保护数据 ADA，用于禁止主微处理器读或者写其中存储了解密密钥的所述存储器的最低地址，还用于禁止主微处理器写其中存储了用户权限的地址，保护根据本发明的存储器的此部分 NVMC2。根据所述保护数据的第二实施例实现包括有条件访问数据的非易失性存储器的此保护。这样，所述部分 NVMC2 是根据图 3 所说明的本发明的原理的非易失性存储器 NVM。

－通过使用外部引导模式自外部存储器下载，对称为安全存储器 NVMS 的集成在芯片上的可编程非易失性存储器进行编程。连接 BUS 可以实现所述下载。依赖于集成在芯片上的安全存储器 NVMS 的大

小，设备的全部程序或者小的引导加载程序存储在该存储器 NVMS 上。此引导加载程序可以在设备启动时检查存储在芯片外部的其他程序段未由黑客修改。为此目的，可以实现外部程序的签名检查，诸如例如，数字签名标准(DSS)、ElGamal 签名、Bos-Chaum 签名、Lamport 签名...。

- 在所述安全存储器 NVMC 的高的地址处设置不同的 MIPS_Protection_Group 特征数据：来自内部非易失性存储器的引导（BOOT_MODE=1）、连接总线的停止（DISABLE_BUS=1）、用于保护下载引导程序的对写入所述安全存储器的授权的限制(READ_ONLY=地址限制）。

- 在所述安全存储器 NVMS 的高的地址处设置不同的 Selection_Options_Group 的特征数据：ENABLE_SECAM、ENABLE_MACROVISION、ENABLE_ICAM、ENABLE_CCIR_OUTPUT。如上文所见，根据本发明的第一实施例，这些选项与 MIPS_Protection_Group 的特征数据相互独立地得到保护。

- 通过改变所述安全存储器 NVMS 的最高地址的 Access_Control_Group 的 Selection_Options_ACCESS_CONTROL 和 MIPS_Protection_ACCESS_CONTROL，保护所述安全非易失性存储器 NVMS。在这样的情况中，密码通常可具有第一安全级，例如，其中最终设备制造商将最终设备递送到广播运营商，广播运营商仍能够通过密码检查(MIPS_Protection_ACCESS_CONTROL=0:1)激活连接总线以测试最终设备。

一旦受到保护，则不存在自芯片去除保护的可能性。所述保护的减弱是不可能的。

通过本发明，芯片制造商仅了解了创建有条件访问系统和创建安全存储器的工具，但是所述芯片制造商未了解算法或密钥。

在需要增补保护的情况中，还可以实现与主芯片相关的智能卡。通过受保护的主芯片，可由公-密钥系统锁住所述智能卡。

这样，根据本发明提供了允许数个保护级别和保护级别的数种组合和并置的完整工具集。单一的可编程非易失性存储器模块可以以独立的方式或者组合的方式，如上文所解释的，提供一个或者数个所给出的实施例、实现方案和应用。这样，本发明满足使保护装置位于芯

片自身上的需要。而且，本发明通过提出可定制的保护装置而获得了更大的成果。

这对于广播运营商和最终设备制造商而言是增补的安全性。这对于芯片制造商而言也是一个优点，其不必在其工厂中沿其物流链引入具体的机密性程序。

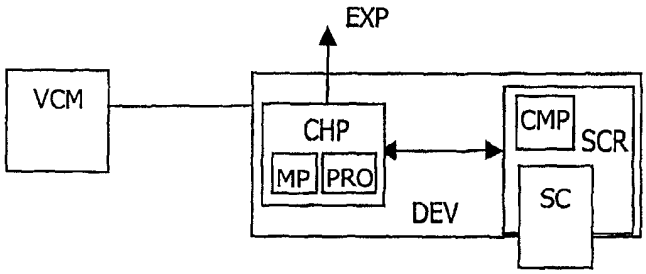

EXP
VCM
CHP
MP
PRO
DEV
CMP
SCR
SC

图 1a

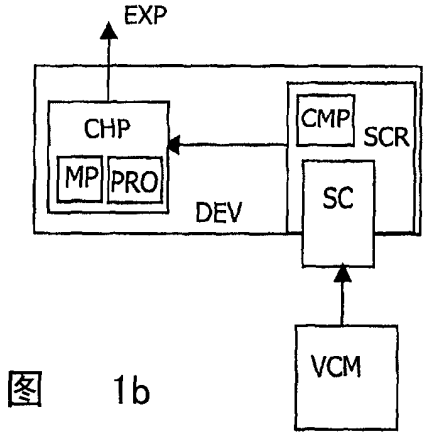

EXP
CHP
MP
PRO
DEV
CMP
SCR
SC
VCM

图 1b

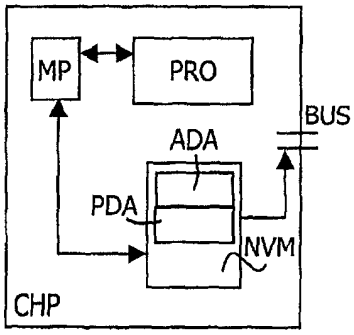

MP
PRO
BUS
ADA
PDA
NVM
CHP

图 2

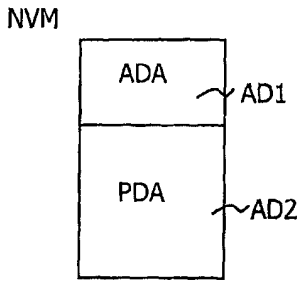

NVM
ADA
AD1
PDA
AD2

图 3

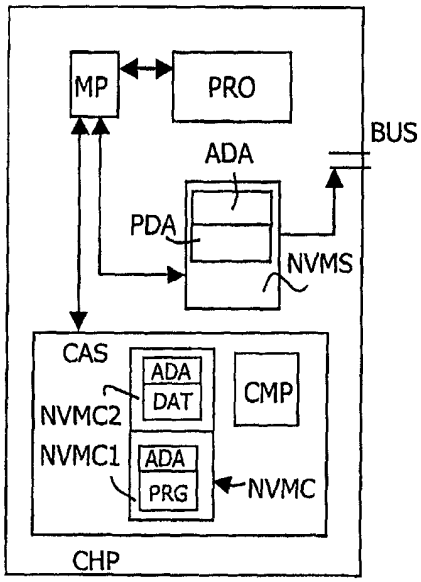

MP
PRO
BUS
ADA
PDA
NVMS
CAS
ADA
DAT
CMP
NVMC2
NVMC1
ADA
PRG
NVMC
CHP

图 4