[19]中华人民共和国专利局

[51]Int.Cl[6]
G07F 7/10

[12] 发明专利申请公开说明书

[21] 申请号 96192241.9

[43]公开日 1998 年 3 月 18 日

[11] 公开号 CN 1176701A

[22]申请日 96.3.6

[30]优先权

[32]95.3.10 [33]DE[31]19508724.0

[86]国际申请 PCT/DE96/00399 96.3.6

[87]国际公布 WO96/28795 德 96.9.19

[85]进入国家阶段日期 97.8.28

[71]申请人 西门子公司

地址 联邦德国慕尼黑

[72]发明人 马库斯·温兰德

[74]专利代理机构 柳沈知识产权律师事务所

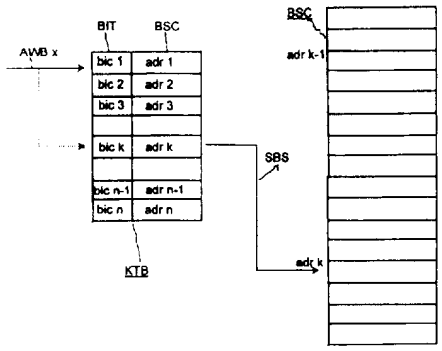
代理人 杨 梧

权利要求书 1 页 说明书 3 页 附图页数 1 页

[54]发明名称 带有保护操作系统的芯片卡

[57]摘要

一种芯片卡，该芯片卡具有至少一个内部处理器和一个非易失的用于处理器的操作系统（BSC）的程序存储器。这些处理器和存储器是这样组织工作的，即芯片卡在其制造和第一次与读写器建立数据技术联系之后仅可执行至少一条指令，该指令用于将操作系统特有的命令表（KTB）补充加载到处理器的非易失的程序存储器内，由此建立起用户指令（AWBx）与操作系统（BSC）中分别执行这些指令的部分的分配关系（adr 1...adr k...adr n）。这样会带来如下优点，即尤其是芯片卡在其被制造到交付给最终用户期间，可防止被非法使用，以及可防止其操作系统被非法查阅和修改。此外还存在以密码逻辑编码的形式来加载命令表（KTB）的方法。



权　利　要　求　书

1. 一种芯片卡，它具有至少一个内部处理器和一个非易失的用于处理器的操作系统(BSC)的程序存储器，这些运算器和存储器是这样组织工作的，即芯片卡在其制造和第一次与读写器建立数据技术联系之后仅可执行至少一条用于将操作系统特有的命令表(KTB)补充加载到处理器的非易失的程序存储器内的指令，由此建立起用户指令(AWBx)与操作系统(BSC)中分别执行这些指令的部分的配置关系(adr 1...adr k...adr n)。

2. 按照权利要求 1 所述的芯片卡，其中具有将命令表(KTB)以密码逻辑编码的形式加载到芯片卡上的方法。

3. 按照权利要求 2 所述的芯片卡，其中密码逻辑编码借助一个校验和来进行。

说　明　书

带有保护操作系统的芯片卡

芯片卡在日常生活的各个领域以强烈上升的势头得到应用。与此相应大量的芯片卡在流通。在芯片卡发行以后，即在其正常使用期间，为了避免特别是卡持有者的财产损失，通常要采取大量措施。例如在卡丢失以后，至少得防止卡被任意第三者擅自使用。

由于芯片卡的数量扩展得很快，为了使特别是大量的芯片卡在分别单独发给最终用户之前已经得到保护，也必须采取措施。例如由卡制造厂家将可能特别多的芯片卡发送给卡的分发者，例如一金融机构。这种途径相当于在银行间运送大量的钱，因此相应地易遭受危险。

在 JP62 - 221089 公开的技术中通过输入数据编码，将其与一个存储在芯片卡上的相对应的数据编码作比较，使芯片卡的封锁在初始化时被撤消。只有当芯片卡上所存储的编码与使用者输入的编码一致的时候卡才被解除锁定进行初始化。在此有一个比较过程。被用来进行比较的数据代码已经包含在卡上了。

由 JP61 - 235994 所公开的芯片卡在初始化时由使用者输入使用者特有的数据。芯片卡包含两个不同的命令组。第一命令组允许进行初始化，当初始化成功结束后通过设置一个所谓的“结束标志”来代替第一命令组，而使第二命令组被启动。由此芯片卡被解除闭锁，供使用者继续使用。

本发明的目的在于对芯片卡提供一种保护，该保护在芯片卡制造后与交付给正常使用期间的中间阶段即生效。由此应该特别排除下列情况，即例如在芯片卡生产过程中加设在芯片卡上的程序密码本身，尤其是操作系统密码能被查阅到，以及密码可能未经许可或非业务性地被修改。

本发明的目的通过权利要求 1 中所提供的芯片卡来实现。

在上述芯片卡中，该内部处理器和一个装有操作系统且非易失(nicht-flüchtigter)的程序存储器相互协调，使得芯片卡在其制造后第一次与读写器建立数据联系的时候，只能执行一条指令，其中操作系统用于处理器和由此可能需要的芯片卡其它功能元件的操作运行，这些功能元件例如是电源，用于

在芯片卡和外部读写器之间交换数据的数据接口等等。该指令将操作系统特有的命令表补充加载到处理器非易失的存储器中。只有在这个加载操作顺利结束后，才有可能将其它的特别是通过芯片卡外部读写器输入的用户指令配置给用于执行该指令的操作系统部分。因而只有在装入命令表之后才能执行属于使芯片卡按规定正常工作的，所有在芯片卡正常使用期间最大限度的可能的操作的指令。

这种执行方式的优点在于，即使有时大量新制造的芯卡片也几乎完全不能使用。对于各芯片卡而言基本上只有在其单独交付给合法的最终顾客之前的那一刻起才能使用。因此新制造的芯片卡不能使用，虽然在其上非易失的存储器和其它的存储区域已经加载了顺序排列的操作系统指令编码，因为由于缺少命令表输入的用户指令无法识别，执行这些指令所必需的操作系统部分由于没有所属的分支地址而不能被激活。实际上以合理的时间和方法几乎不可能以一种“反求工程”的方式去重建操作系统的功能结构，从而以进入地址的方式获得执行单个用户指令的部分及其可能的相互作用。

本发明芯片卡的这种设计有这样的优点，即在通过将芯片卡交付给新的所有者使用之前的那一刻补充加载命令表而授予用户使用权之前，几乎可防止任何形式的非法使用，而不必在芯片卡的硬件和软件区域内采取昂贵的，使得芯片卡的制造费用提高和可能使其使用功能受到限制的种种措施。一方面可以简单的方式使芯片卡能单独执行加载命令表的指令。另一方面命令表的补充加载对于一个合法地拥有命令表编码的机构，例如一个银行来说，不存在任何数据技术方面的问题。在这个过程中若需要也可以同时传送一些其它的例如使新用户的芯片卡具有个人特色的数据。

通过本发明，除了阻止芯片卡在其交付正常使用之前被无权使用以外，也防止了在此中间阶段在生产过程中加设在芯片卡上的程序编码，尤其是操作系统编码以未经许可的方式被查阅，以及未经许可或非业务性地被修改。

按照本发明的另一有利改进方案，可采取辅助手段，使命令表的传送以密码逻辑编码的形式进行。在加载过程中虽然传送的命令表的编码指令序列可能被窃听，然而，命令表也不会成为可能的非法使用者手中的明文。密码逻辑编码通过一种所谓的校验和而有利地得到保护。

下面借助附图所示实施例对本发明作进一步的详细说明。

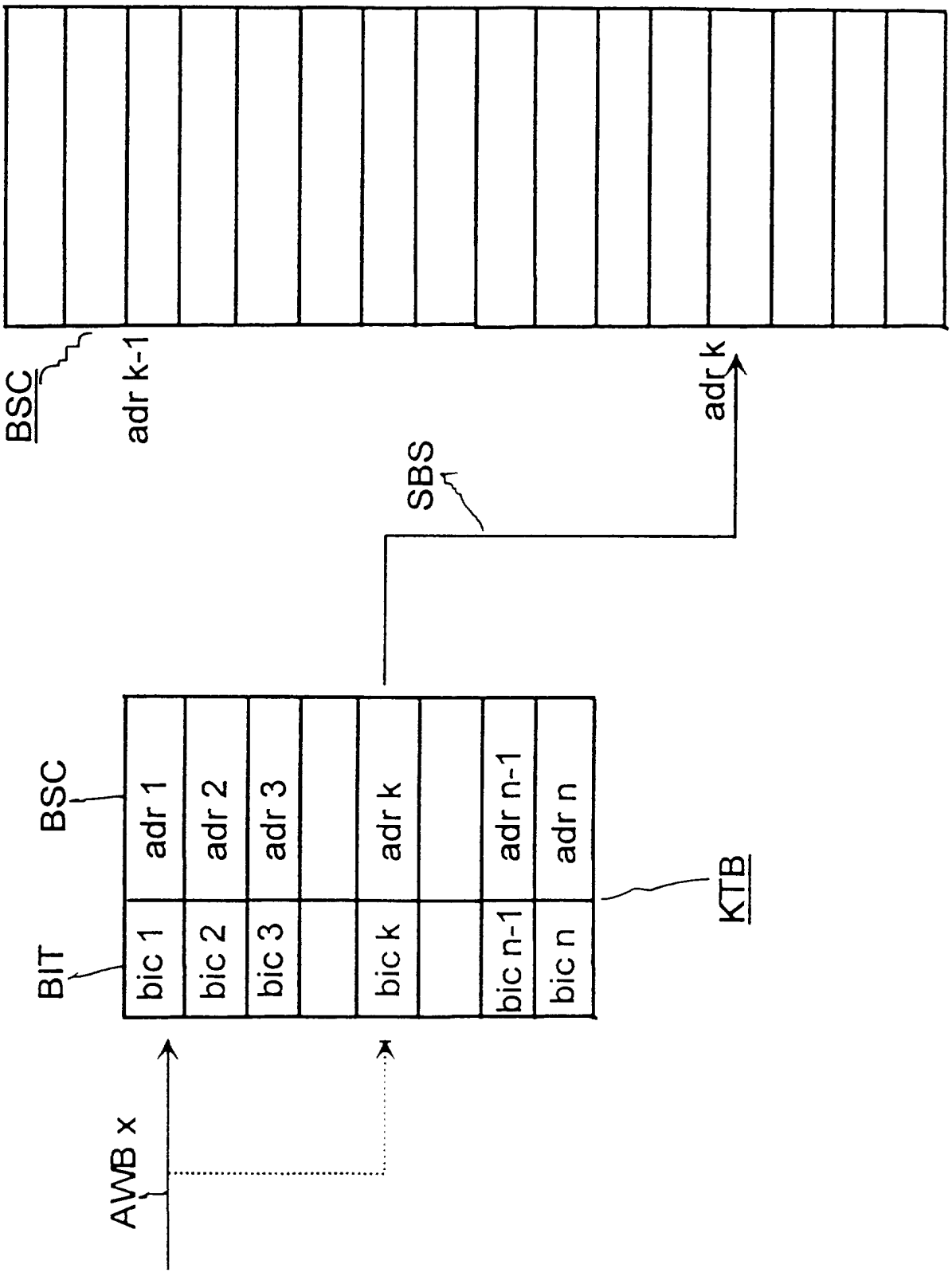
在图的右侧示例地以直观的表格形式示出连续排列的操作系统编码

(BSC)的局部序列中的一段。在此，可以想象表格不仅向上而且也向下延伸。这段序列示出了前面的进入地址 adr k - 1 和其后紧跟着的进入地址 adr k。分配给这些进入地址其中一个的操作系统指令行与紧跟其后直至下一个进入地址的那些指令行构成一组，这组指令用于执行一确定用户命令。

在图示实施例中，优选通过一个外部读写器将一个当前用户命令 AWB x 传输给芯片卡。这个过程由操作系统执行。为此需要一命令表 KTB，该命令表宛如一把能打开操作系统 BSC 功能部分入口的钥匙。在实施例中命令表 KTB 的每一行由第一编码段 bic k 和第二编码段 adr k 组成，其中第一代码段 bic k 用于识别，即用于当前用户命令 AWB x 类型的识别，而第二代码段包含有所属操作系统指令序列的起始地址。因此命令表 KTB 由第一部分表 BIT 和第二部分表 BSC 组成，其中第一部分表包含用于判读指令的编码 bic1, bic2, bic3, ...bic k, ...bic n - 1, bic n，第二部分表 BSC 包含附属于相应操作系统序列的进入地址 adr1, adr2, adr3...adr k...adr n - 1, adrn。

在图示实施例中，一个用 AWB x 表示的用户命令传输给芯片卡。该命令通过编码 bic k 被认作为许可命令，在图中命令表 KTB 左侧用虚线来表示这一点。接着与此有关的进入地址 adr k 被激活，由此操作系统 BSC 编码从进入地址 adr k 处开始被执行。在图中通过一个从命令表 KTB 相对应行到进入地址 adr k 的箭头 SBS 来表示对属于用户命令 AWB x 的操作系统序列的调用。

由示图可以看出，没有命令表 KTB 的搭桥作用就不能执行用户命令 AWB x，因为不可能将用户命令 AWB x 分配给操作系统中与此相关的部分。因此按照本发明设计的芯片卡能够特别有效地防止新制造的芯片卡被非法使用。


BSC
adr k-1
adr k
SBS
BSC
adr 1
adr 2
adr 3
adr k
adr n-1
adr n
BIT
bic 1
bic 2
bic 3
bic k
bic n-1
bic n
KTB
AWB x