[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公开说明书

[21] 申请号 01806552.X

[43] 公开日 2003 年 5 月 14 日

[11] 公开号 CN 1418356A

[22] 申请日 2001.1.12 [21] 申请号 01806552.X
[30] 优先权
[32] 2000. 1.14 [33] FR [31] 00/00488
[86] 国际申请 PCT/FR01/00110 2001.1.12
[87] 国际公布 WO01/52201 法 2001.7.19
[85] 进入国家阶段日期 2002.9.13
[71] 申请人 梅姆普拉斯公司
地址 法国热姆诺
[72] 发明人 C·比丹 P·吉拉德
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 崔幼平 黄力行

权利要求书 2 页 说明书 5 页 附图 1 页

[54] 发明名称 保护多用途智能卡中的个人身份号码以防止失窃的方法和实现这种方法的芯片卡

[57] 摘要

本发明涉及到通过尚未访问到外部的应用保护多用途智能卡的 PIN 号码以防止失窃的方法。 本发明的方法包括利用避免访问到卡的外部的一种或多种应用检测 PIN 号码核查的操作，无论应用如何都对不成功试探的次数计数，在连续试探的操作次数达到预定界限值时就阻止上述卡的操作。

ISSN1008-4274

1.一种用于保护多用途芯片卡的密码以防止失窃的方法，其特征是，用尚未访问到卡的外部的一种或多种应用检测密码核查的操作，并且当检测的操作次数达到了预定界限值的时候，阻止所述卡或所述一种或多种应用的运行。

2.根据权利要求1所述的用于保护密码以防止失窃的方法，其特征是，密码核查操作的检测包括触发至少一个批准计数器，以便对不成功的密码试探进行计数。

3.根据权利要求1或2所述的用于保护密码以防止失窃的方法，其特征是，采用两个批准计数器，第一计数器用于对不成功的试探进行计数，在达到可能出示的预定最大次数之前，所述计数器在持有者出示正确密码时被复位到零，在相反情况下就阻止卡的运行，并且每当第一计数器接近最大值时使第二计数器增值，并且在这个第二计数器的值达到预定界限值时阻止卡的运行。

4.根据权利要求1或2所述的防止密码失窃的方法，其特征是，对每一种应用采用一个批准计数器，每个计数器能够对涉及每一种易于被卡使用的应用的不成功的密码试探进行计数，只要有一个计数器达到用于所述计数器的预定界限值就导致阻止卡的运行。

5.一种多用途芯片卡，其特征是，其具有对尚未访问到外部的应用检测密码核查操作的装置，以及在核查操作次数达到预定界限值时阻止其运行的装置。

6.根据权利要求5所述的多用途智能卡，其特征是，检测密码核查操作的装置包括至少两个批准计数器，用于对不成功的密码试探进行计数。

7.根据权利要求6所述的多用途芯片卡，其特征是，第一计数器能够对不成功的试探进行计数，在达到可能出示的预定最大次数之前，所述计数器在持有者出示正确密码时被复位到零，在相反情况下就阻止卡的运行，并且每当第一计数器接近最大值时使第二计数器增值，并且在这个计数器的值达到预定最大值时由阻止装置使用该第二计数器，以便阻止卡的运行。

8.根据权利要求5所述的多用途芯片卡，其特征是，批准计数装置包括每一种应用的一个计数器，每个计数器能够对涉及每一种易于被

卡使用的应用的不成功的密码试探进行计数，只要有一个计数器达到用于所述计数器的预定界限值就导致阻止卡或应用的运行。

保护多用途智能卡中的个人身份号码以防止失窃的方法和实现这种方法的芯片卡

本发明涉及到保护多用途芯片卡中的密码防止失窃的方法。还涉及到采用上述方法的芯片卡。

多用途芯片卡意味着卡中包含一个或多个集成电路芯片，所述的卡在卡的有效期限内能够执行各种装载或卸载的应用程序。

在现有的多用途智能卡解决方案当中，可以举出的例子有Sun公司所定义/规定的“JavaCard”或Microsoft公司所定义/规定的“SmartCard for Windows”。

为了简明，以下要说的应用是指应用程序(或者是英语词汇的小应用程序)。

密码是指持卡人的个人身份号码，也被称作PIN号码(个人身份号码)。

为了与仅仅支持一种应用的芯片卡兼容，并且简化卡的使用，多用途芯片卡通常对所有应用采用一个通用的PIN号码。也就是VISA所制定的OP规范，目前可作为装载/卸载以及多用途芯片卡应用的内部管理的标准，它为智能卡现有和未来的所有应用限定了唯一的密码。

在多用途卡的应用中出现的问题在于，卡是为了在其整个寿命过程中装载或卸载新应用而设计的。这在理论上是有益的，但这种特性在实践中会使卡易于损坏，因为恶意应用可以以对持卡人不可见的方式与其它应用一起装载。因此对这种应用的开放在实践中当然会泄漏卡的密码。

从这一点来看，申请人发现有可能用这样一种攻击方式查找卡的PIN号码:

这种攻击假设存在没有能进入对卡进行处理的终端的一种恶意应用，也就是说没有达到与外部对话的目的。

只要不存在可能用协议与这种应用直接对话的任何终端，这种应用就没有机会访问一个终端。尽管如此，这种应用还是能在卡内执行，因为它是为卡的其它应用提供/供应服务。例如有可能用于信用度应用，这种应用被指定用于信用度点计数。

在攻击过程中利用不能与外部对话的一种应用按以下程序执行。

这种应用实际上是利用操作系统(或是一种专用应用)提供的逻辑接口,并且有可能核查密码。对于VOP,“JavaCard”的OP方式,这一接口是“核查PIN”操作。

能够与外部对话并且希望核查持卡人标识符的一种应用是通过在芯片卡所插入的终端屏幕上显示一个信息来请求用户输入他的密码。然后这种应用用操作系统(或是一种专用应用)提供的接口来核查用户输入的值是否与卡的密码值相同。如果相同,操作系统(或是可以响应密码核查的应用)就给出确认响应;或是在相反情况下拒绝。

由于密码核查接口可以接受所有应用的卡,恶意应用也能触发执行这种操作,并且能测试各种值直至获得指示当前密码有效的正确响应。

这样,恶意应用就能利用密码核查操作(为VOP核查PIN)并且试探各种值的密码(0,01,02,03,...9999)。

为了防止有人测试大量的值,卡上通常具有一个批准计数器,在达到给定次数的错码时阻止操作。实际使用的次数通常是3次。

因此,恶意应用有可能连续提供两个码值(更普遍的情况是,如果造成卡被阻止的错码次数是n,也就是n-1),如果错码两次,也就是对密码核查的响应是否认,批准计数器就会增加二,应用就按设计要求停止测试,并一直等到用户输入正确的码使计数器重新初始化。

如上所述,这是因为由一项与外部对话的应用对话的用户进行的触发使用密码核查程序。请求用户从终端键盘上输入密码。执行核查程序,如果用户没有错误,由于恶意应用的试探达到2的批准计数器就被复位到零。这样就能重新测试恶意应用。

本发明的目的是解决这种问题。

本发明的主题是一种保护多用途芯片卡的密码防止失窃的方法,其特征是,包括用尚未访问到卡的外部的一种或多种应用检测密码核查的操作,当检测的操作次数达到了预定界限值,就阻止上述卡或上述一种或多种应用的运行。

根据本发明的一个特征,密码核查操作的检测包括触发批准计数器对不成功的密码试探计数。

根据第一实施例，该方法包括采用两个批准计数器，第一计数器对不成功的试探计数，在达到可能出示的最大预定次数之前，上述计数器在持卡人出示正确密码时被复位到零，在相反情况下就阻止卡的执行，并且包括每当第一计数器接近最大值时将一个第二计数器增量计数，并且在第二计数器的值达到预定界限值时阻止卡或这种应用的运行。

根据另一个实施例，该方法包括对每一种应用采用一个批准计数器，每个计数器能够对涉及每一种易于被卡使用的应用的不成功的密码试探增量计数，只要有一个计数器达到这一计数器的预定界限值就立即阻止卡的运行。

本发明的另一主题是一种多用途芯片卡，其特征在于它具有用尚未访问到卡的外部的应用检测密码核查操作的装置，以及在核查操作次数达到预定界限值时阻止执行核查操作的装置。

检测密码核查操作的装置包括至少两个批准计数器，用于对不成功的密码试探计数。

根据第一实施例，计数装置包括两个批准计数器，第一计数器对不成功的试探计数，在达到可能出示的最大预定次数之前，上述计数器在持卡人出示正确密码时被复位到零，在相反情况下就阻止卡的运行，并且每当第一计数器接近最大值时将一个第二计数器增量计数，并且在第二计数器的值达到预定最大值时由阻止装置使用该第二计数器，以便阻止卡的运行。

根据另一个实施例，批准计数装置包括每一种应用一个计数器，每个计数器能够对涉及每一种易于被卡使用的应用的不成功的密码试探增量计数，只要有一个计数器达到这一计数器的预定界限值就阻止卡或应用的运行。

阅读以下参照附图提供的说明就能理解本发明的其它特征及其优点，在附图中：

图1表示一种多用途芯片卡的运行框图，

图2表示第一实施例的运行框图，

图3表示第二实施例的运行框图。

为了说明在实现本发明方法时采用的不同元件，在图1中表示了一种多用途芯片卡的示意图。

根据本方法所建议的第一方案包括采用两个批准计数器，第一计数器不论应用对所有失败的密码键入计数，在达到可能出示的预定最大值之前，在出示了正确的密码时，上述计数器就被复位到零，在相反情况下就阻止卡的执行，第二计数器对第一计数器超过预定界限值的次数计数，第二计数器在出示正确密码之后不被复位到零。

第二种方案包括对每一种应用A1，A2，...，An采用一个批准计数器。

为了便于理解本发明，所述的芯片卡具有一个带程序储存器的处理单元U，其中有卡的操作系统以及一些应用，这些应用能够利用其它应用的接口向其它应用提供服务来扩展由操作系统提供的运行，例如是专用于核查密码的应用。

各种应用程序A1，A2，An可以存储在同一个程序存储器M1中，或是存储在用于此目的的另一个程序存储器M2中，以便能够在卡的有效期间装载新的应用。这种存储器可以是(EEPROM型的)电可擦除存储器。

在存储器M2中可以提供一个对不成功试探计数的区域Z。

根据图2所示的第一实施例，由尚未访问到外部的一种应用执行的对不成功试探的检测是利用两个计数器CP1和CP2来执行的。

在任何一个应用运行的核查程序执行完核查并且出现了错误密码的情况下，计数器CP1就被增值。这样，在一个应用尚未访问到外部的情况下，为核查所提供的密码只能来自这种应用，该应用试探着发现密码。

在应用已经访问到外部的情况下，该应用就请求持卡人提供用于核查密码的代码。从理论上说，持卡人出错的可能性往往比试图发现密码的恶意应用要小。

本发明建议使用二级批准计数器CP2。它包括不对已经出现的错码次数进行计数，但是对第一计数器CP1的值接近致使阻止执行的值的次数进行计数。

根据实际情况，每当出现错码时，第一计数器CP1就增值，无论错码是由持卡人还是恶意应用执行的。这一计数器的最大值例如是3(3次可能的试探)。如果在这3次试探中输入了正确的密码，计数器CP1就被复位到零。当这一计数器的值接近最大值也就是在本例中的2时，第二计数器CP2就增值。

这样，每当第一批准计数器通过2(如果阻止值例如是3)，第二计数器就计数。第二计数器不会复位到零，当它的值达到预定界限值N′时，系统就阻止卡的运行。

为第二计数器确定的界限可以根据密码的长度来选择。码越长，用户在按键时可能发生的错误就越多，在这种情况下可以选择比码较短时更高的界限值(例如是4位数字)。

根据图3所示框图建议和表示的第二种方案，为每一种应用提供一个批准计数器，CP1用于A1，CP2用于A2，...，CPn用于An(n种应用)。密码用统一的，也就是对所有应用采用同样的密码，但是每种应用有一个相关联的计数器。

每当输入错码时，对应该应用的计数器就随之增值。当输入的密码正确时，该应用的计数器就复位到零。当计数器值达到最大值(例如是3)时，就阻止卡或该应用的运行。这种机制对卡中的所有应用都一视同仁。当一个新的应用被装载到卡中时，操作系统就将一个计数器与这一新的应用相关联。

操作系统借助于标识字段AID(小应用程序标识符)来识别每一种应用。

随着对每一种应用的识别，操作系统联系到对应的批准计数器，并且每当出现一个错码时就将其增值。对于执行不成功密码试探的尚未访问到外部的恶意应用，就要求提供密码。

对于其它应用，要求持卡人在终端键盘上输入他的密码。

这样，恶意应用就无法三次以上提供错误密码了(如果计数器被固定在3)。

图 1

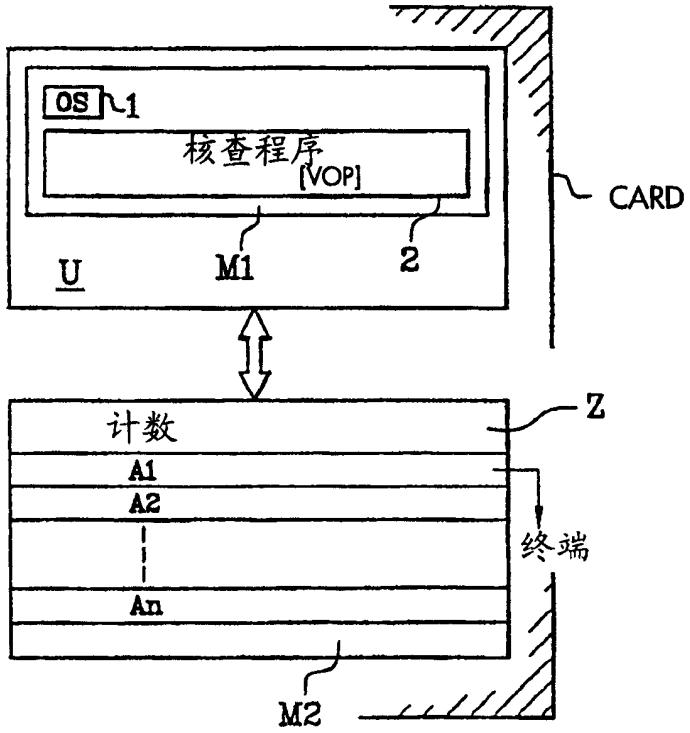

OS
1
核查程序
[VOP]
CARD
U
M1
2
计数
Z
A1
A2
An
终端
M2

图 2

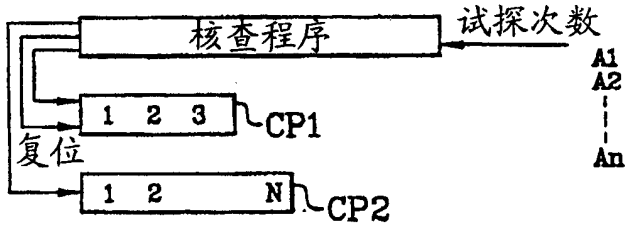
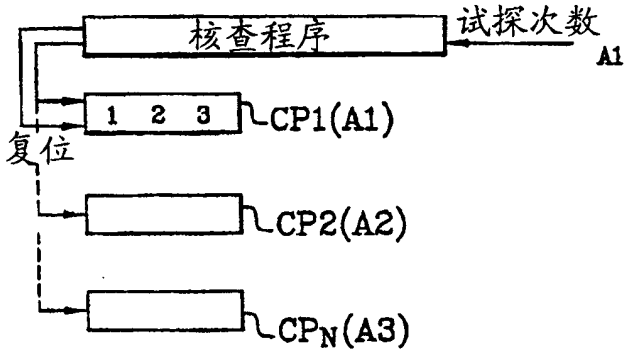

核查程序
试探次数
A1
A2
An
1 2 3
CP1
复位
1 2 N
CP2

图 3


核查程序
试探次数
A1
1 2 3
CP1(A1)
复位
CP2(A2)
CPN(A3)