



[12] 发明专利说明书

[21] ZL 专利号 94108891.X

[45] 授权公告日 2003 年 12 月 24 日

[11] 授权公告号 CN 1132128C

[22] 申请日 1994.6.7 [21] 申请号 94108891.X

[30] 优先权

[32] 1993.6.8 [33] FR [31] 9306855

[71] 专利权人 布尔 CP8 公司

地址 法国卢福西内

[72] 发明人 雅克·帕特瑞

审查员 杨勤之

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

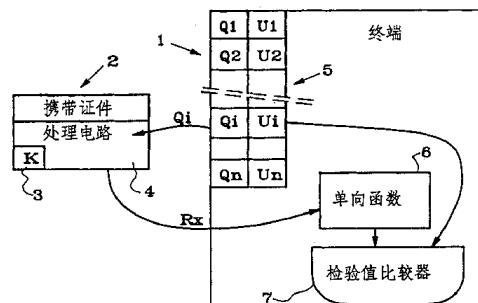
代理人 杨国旭

权利要求书 4 页 说明书 10 页 附图 2 页

[54] 发明名称 由离线终端认证携带证件的方法，相
应的携带证件及终端

[57] 摘要

本发明涉及由离线终端(1)认证一种包含处理电路(4)的携带证件(2)的方法，该处理电路用于提供一个作为由终端发出的一次数值(Q_i)函数的二次数值(R_i)。在终端中设置了一个组合有一系列一次数值(Q_i)及一系列检验数值(U_i)的认证表格(5)，当一个携带证件与终端相连接时，传送给携带证件一个表格中的一次数值(Q_i)，并对从携带证件接收到的二次数值(R_x)运用单向函数计算，并将获得的结果与表格中相应的检验值相比较。



1.由一个离线终端对一系列便携物中的一个便携物进行鉴别的一种方法，所述便携物存储有一种密码（K）且所述终端存储有一种单向函数，所述方法包括以下步骤：

给所述终端设置一个鉴别表，该鉴别表与一系列的一次值（Qi）和一系列的控制值（Ui）相关，且所述鉴别表，是通过把在一个可靠的便携物上的每一个一次值（Qi）与它的所述密码（K）一起进行处理以导出一个二次值（Ri）并在一个被授权的机构的一个设备中借助所述单向函数对所述二次值（Ri）进行处理以导出所述控制值（Ui），而为所述终端设置的；

把所要鉴别的所述便携物连接到所述离线终端；

把所述一次值（Qi）之一从所述终端发送到所述便携物；

把所述便携物中的所述一个一次值（Qi）与其密码（K）一起进行处理，以导出一个二次值（Rx）；

把所述二次值（Rx）从所述便携物发送到所述终端；

在所述终端中把所述单向函数应用于从所述便携物接收的所述二次值（Rx）以导出一个函数结果；以及

在所述离线终端中把所述函数结果与所述鉴别表中与所述一个一次值（Qi）相应的一个控制值（Ui）进行比较。

2.根据权利要求1的方法，其中给所述终端设置一个鉴别表的步骤进一步包括以下步骤：

形成一个一次值（Qi）与一个相应的控制值（Ui）的一个第一结合；

借助一种非对称函数对该第一结合进行加密以形成一个对应的签名值 (Si)；以及

把该对应的签名值 (Si) 存储在所述鉴别表 (5) 中，且比较所述函数结果的步骤进一步包括以下步骤：

通过应用所述非对称函数的一个反函数，对所述对应的签名值 (Si) 进行解密，以形成一个解密的签名值；

把所述一次值 (Qi) 与所述鉴别表的所述对应的控制值 (Ui) 相结合，以形成一个第二结合；以及

把该解密的签名值与所述第二结合进行比较。

3.根据权利要求 1 的方法，进一步包括以下步骤：

在已经向一个便携物发送了一次所述一次值之后，从所述终端的所述表中消除各个一次值。

4.根据权利要求 1 的方法，其中发送所述一次值之一的所述步骤进一步包括以下步骤：

把一个预定的表的一个表标识符链接到该表的每一个一次值；

在所述便携物的存储器中记录表明从其中已经发送了所述一次值的表的表标识符；

在所述便携物中为每一个表标识符设置一个计数器，以对从该表至所述便携物的每一次一次值发送进行计数；以及

当在所述便携物中接收到使为所述表设置的计数器达到一个存储的阈值的一个一次值时，阻止从所述便携物向所述终端发送一个二次值，其中所述一次值来自所述表。

5.根据权利要求 4 的方法，其中所述计数步骤进一步包括以下

步骤：

把各个便携物中与所述终端中的一个修正的表相对应的所述计数器复位至零。

6.根据权利要求4的方法，其中在向所述便携物发送一个一次值的步骤之前，包括检验所述一次值所包含的所述表标识符对应于之中存储有所要发送的一次值的所述表的步骤。

7.根据权利要求1的方法，其中多个密码(K)中的每一个密码(K)被分布在所述一系列的便携物中的各个便携物中，为所述终端提供一个鉴别表的所述步骤包括提供若干个表，该若干个表中的每一个表都存储基于一个公共密码(K)的那些控制值(U_i)，且把所述一次值(Q_i)之一发送到所述便携物的步骤包括：

从一个第一便携物向所述终端发送与所述第一便携物的一个第一密码相关的一个第一表，用于进行识别；

把所述识别的第一表的所述一次值(Q_i)之一从所述终端发送至所述第一便携物。

8.用于在一种离线模式下对一系列便携物中的一个便携物进行鉴别的一种终端，包括：

一个鉴别表，该鉴别表把一系列的一次值(Q_i)与一系列的控制值(U_i)相联系，所述控制值(U_i)，是通过在一个可靠的便携物的处理电路中把每一个一次值(Q_i)与它的一个密码(K)进行处理以导出一个二次值(R_i)并在一个被授权的机构的处理电路中借助一个单向函数对所述二次值(R_i)进行处理以导出所述控制值(U_i)，而被导出的；

一个处理电路，用于在向所要鉴别的所述便携物发送了所述

一次值 (Q_i) 之一之后，把所述单向函数应用至从所述便携物接收的一个二次值 (R_x)，以导出一个函数结果；以及

一个比较器，它与所述表和所述处理电路相连通，以把所述函数结果与所述鉴别表中同所述一个一次值 (Q_i) 相对应的一个控制值 (U_i) 进行比较。

由离线终端认证携带证件的方法，
相应的携带证件及终端

本发明涉及一种由线外终端认证携带证件的方法以及可采用该方法的携带证件和终端。

离线终端应被理解成在不与一个中心机构相连接的情况下即可对携带证件进行认证的终端。

我们知道，由信息装置提供的福利或服务正面临着越来越大的发展。由一个网所提供的福利或服务接口是由携带证件与其相连接的终端来执行的，该携带证件通常是由主管(授权)机关发给的存储卡。在与福利或服务接口之前，必须使每个终端能认证与它相连接的携带证件，以便当该证件不是由该主管机关发给的就拒绝该携带证件。

一种公知的认证方法在于，使每个终端与一个中心认证机构相连接，以便执行联机认证，而中心认证机构应作出防护以便阻止行骗者接通接口，这些行骗者想利用不是该授权机关发给的证件通过认证。然而这样一种方法是很昂贵的，因为要用大的通信网持续地在各终端与中心认证机构之间工作。

为了降低认证费用，终端常作成离线的，并在每个终端中设

置可以使其进行认证的程序。

现在已经公知了两种由离线终端认证的方法。根据第一种方法，终端包含一种密码并开发了一种利用这种密码的计算方法。但是这些终端往往指定设置在很难受到完全防盗保护的地方，并易被行骗者窃取密码，从而使其可能制作出由包含同样密码的其它终端所认证的携带证件。因此必须设置昂贵的装置用来有效地保护密码。

根据第二种公知方法，离线终端包括一种可存取的码，但必须在携带证件中设置一种使用模数乘法的数字计算法，这就意味着在携带证件中设置通常是非常昂贵的处理电路。

本发明的目的在于提出一种能由不包含密码的离线终端所采用的方法，而且不需要由携带证件的处理电路执行这些模数的乘法运算。

为了实现该目的，根据本发明提出了一种由离线终端认证带有处理电路的携带证件的一种方法，该处理电路用于提供一个二次数值，它是由终端发出的一次数值的函数，其特征在于：在终端中设置了一个组合着一系列一次数值及一系列检验数值的认证表格，每个检验数值都是由被认证携带证件的处理电路计算的二次数值单向函数的转换值(变式)；特征还在于，当一个携带证件与终端相连接时，传送给携带证件一个表格中的一次数值，并对从携带证件接收到的二次数值运用单向函数计算，并且将获得的结果与表格中相应的检验值相比较。

因此，对于接近到表格的行骗者来说不可能根据检验值来确定二次数值，该二次数值需由携带证件来提供，以使得由单向函

数对二次数值的转换值与表格中的检验值相同。

本发明也涉及到适用于实施上述方法的一种携带证件及一种终端。

根据本发明的一个方面，提供了由一个离线终端对一系列便携物中的一个便携物进行鉴别的一种方法，所述便携物存储有一种密码且所述终端存储有一种单向函数，所述方法包括以下步骤：

给所述终端设置一个鉴别表，该鉴别表与一系列的一次值和一系列的控制值相关，且所述鉴别表，是通过把在一个可靠的便携物上的每一个一次值与它的所述密码一起进行处理以导出一个二次值并在一个被授权的机构的一个设备借助所述单向函数对所述二次值进行处理以导出所述控制值，而为所述终端设置的；

把所要鉴别的所述便携物连接到所述离线终端；

把所述一次值之一从所述终端发送到所述便携物；

把所述便携物中的所述一个一次值与其密码一起进行处理，以导出一个二次值；

把所述二次值从所述便携物发送到所述终端；

在所述终端中把所述单向函数应用于从所述便携物接收的所述二次值以导出一个函数结果；以及

在所述离线终端中把所述函数结果与所述鉴别表中与所述一个一次值相应的一个控制值进行比较。

根据本发明的另一个方面，提供了用于在一种离线模式下对一系列便携物中的一个便携物进行鉴别的一种终端，包括：

一个鉴别表，该鉴别表把一系列的一次值与一系列的控制值

相联系，所述控制值，是通过在一个可靠的便携物的处理电路中把每一个一次值与它的一个密码进行处理以导出一个二次值并通过在一个被授权的机构的处理电路中通过一个单向函数对所述二次值进行处理以导出所述控制值，而被导出的；

一个处理电路，用于在向所要鉴别的所述便携物发送了所述一次值之一之后，把所述单向函数应用至从所述便携物接收的一个二次值，以导出一个函数结果；以及

一个比较器，它与所述表和所述处理电路相连通，以把所述函数结果与所述鉴别表中同所述一个一次值相对应的一个控制值进行比较。

本发明的其它特征与优点在阅读了以下结合附图对本发明各种方法的说明后将会被清楚地了解，其附图为：

图 1 以图解形式说明了本发明方法的第一种方案；

图 2 是比图 1 中所示方法更加复杂的一种方法的图解形式；

图 3 以图解方式表示出本发明一种有利变形，它与相同于图 1 所示的本发明方法变型有关；

图 4 以图解形式描述了图 3 所示方法的一种实施变型。

参照图 1，本发明的方法指定用于由一个通常标号为 1 的离线终端认证一个通常标号为 2 的携带证件，该携带证件包括一个不能从携带证件外部读出的存储器 3，而且包含一个认证密码 K 还包括一个本身公知的对称编码算法的处理电路 4，该算法通常是一种复杂的计算方法，用于提供二次数值 R_i 它是密码 K 及终端发出的一次数值 Q_i 的函数。在本发明的第一种实施变型中，密码 K 对于所有可

与终端连接的携带证件均是相同的。

在以下的说明中，用“问题”一词来代表一次数值 Q_i ，而用“回答”一词来代表二次数值 R_i 。

作为一个非限制性的例子，该对称的编码算法例如是一种公知的名称为“数据标准编码”（“DATA ENCRYPTION STANDARD”）简称为DES的算法，以便由公式 $R_i = DESK(Q_i)$ 来对问题 Q_i 给出回答。

此外，在该终端1中设置了一个包括一系列问题 $Q_1, Q_2, \dots, Q_i, \dots, Q_n$ 及一系列检验数值 $U_1, U_2, \dots, U_i, \dots, U_n$ 的表格5，这些检验数值是由受认证的携带证件中处理电路计算的回答 $R_1, R_2, \dots, R_i, \dots, R_n$ 的单向函数转换值。因而有 $U_i = f(R_i)$ 。该单向函数 f 例如是对平方数按模 m 的计算，其中 m 是两个保密大质数的乘积。

对于问题 Q_i ，因此有检验值：

$$U_i = (R_i)^2 \bmod m.$$

在本文中单向函数是指在没有专门信息的方向上可被计算而在相反的方向上不可被计算的一种函数。在所述实例中，事实上只能在知道 R_i 时计算 $(R_i)^2 \bmod m$ ，而不能在仅知道 U_i 时确定出 R_i 。

在本发明的方法中，检验数值由主权机构依次地应用单向函数由被认证的携带证件对预计在表格中要存入的不同问题的不同回答计算出来，然后将所有的问题及检验数值装入到终端的表格中。每个终端可具有其专有的问题 Q_1, \dots, Q_n 。

此外，终端1包括一个处理电路6，它运用同样的单向函数，在被认证的携带证件与终端相连接及被发送给该证件一个问题 Q_i 时对携带证件给出的回答 R_X 进行计算。该终端1同时包括一个比较

器7。它将表格中与问题Qi相对应的检验数值Ui与回答Rx被单向函数转换的值相比较，该回答Rx是由携带证件对发送给它的问题Qi作出的回答。

如果被连接的携带证件得到认可，则回答Rx等于Ri，其被单向函数转换的值因而等于Ui。这时该终端进入到与所考虑的携带证件相关的预定操作。相反地如果携带证件没有被认可，则回答Rx不等于数值Ri，并使得其单向函数转换值不同于检验数值Ui，故携带证件被拒绝。应当注意到，在该方法中对表格5的取数可以是公开的，而这会使人产生在终端中没有一个包括回答R1, R2, ..., Ri, ..., Rn的表格的错觉，因为这时对于行骗者来说易于制作一个既不包括密码K又不包括对称处理电路的携带证件，而其中仅包括一个与表格5相同的表格，以便在终端发出一个问题Qi时向终端发回一个回答Ri。还应该注意到，对于已取得表格5数据的行骗者也不可能发现出回答Ri的值，因为要确定出这种回答值必须以能使函数 $Ui=f(Ri)$ 逆向运算为前提。应该指出，在该方法中单向函数f是一个绝对的单向函数，也就是说实际上不存在任何对函数f可逆向计算的函数，或如同所述实例中那样，f是对平方数按模m计算的函数，这是一种仅在知道某些参数时才可逆向运算的函数，但实际上是不可能可逆运算的，因为这些参数没有包含在终端中。

由于终端1可达到的特性，本发明方法最简单的形式不能保证力求达到的可靠性，这种可靠性是针对那些不仅可能查阅表格5而且能在别人不注意时对其作出修改的人。事实上对于这种人，他一方面可以作出一个伪携带证件，该证件中包括一个对终端的提问发回答的某种算法；另一方面对终端中表格5的检验数值作

出修改，以使得这些检验数值能够等于对伪携带证件提供的回答运用单向函数运算的结果。事实上在该所述情况下，由比较器7作出的比较结果肯定会满足要求并由此可使其进入到由终端控制的操作中。为了防止这种诈骗，预设了一种根据本发明方法的更为复杂的形式，它被示于图2中。

在本发明的第二种形式中，终端包含一个表格5，表中不仅包括如前述的一系列问题及一系列检验数值，而且另外还包括一系列的标记值 $S_1, S_2, \dots, S_i, \dots, S_n$ ，这些值是问题及相应的检验数值组合的一种非对称译码函数的转换值。一个问题 Q_i 例如是一个64位数串，而检验数值 U_i 例如是一个128位数串，对问题及检验数值的组合例如是这样实现的：将问题及检验数值的双重数串根据顺序 $Q_i \ U_i \ Q_i \ U_i$ 连接起来，然后用非对称译码函数由主权机构对这个组合作出运算，以便确定出收入到认证表格5中的相应标记值 S_i 。该非对称译(成密)码函数例如是对得到的组合数平方根值的按模 m 的计算。这种平方根值的按模 m 的计算只有在知道一些参数时才能确定，这些参数无论如何是不会包括在终端中的。

当认证一个证件时，一方面运用上面关于本发明方法简单方式所述程序，如果回答是正确的，则借助一个处理电路8在终端中执行上述组合 $Q_i \ U_i \ Q_i \ U_i$ ，并借助一个处理电路9对标记值 S_i 运用非对称译(成密)码函数的反函数计算，该非对称译码函数就是主权机关用来确定标记值 S_i 所使用的函数，然后在一个比较器 10 中将被处理电路8作出的组合数与被处理电路转换的标记数值 S_i 的转换值相比较。应当注意到，这种非对称反函数即所述例中是对平方值的按模 m 的计算无须要知道参数值，而这些参数值在运用直

接的非对称译码函数时是必须知道的。由终端实现的这种反函数可能被一个行骗者理解，因此这不能使行骗者确定出必须与一个检验值同时输入的标记值，以便使该标记值能与检验值紧密相关。尤其是，如已经预见到的，行骗者制作出一伪证件，并篡改相应的检验数值以使得第一次比较能够满足，但对他来说却不能确定出为使第二次比较也满足而应与该检验数值相组合的标记值。因此这种方法与本发明最简单方式相比安全性得到了改善。

对于一个深思熟虑的行骗者来说同样可作到不用修改终端中的表格5，而是假定获得一个认证的卡，并连续地利用发送表格中的所有问题及在运用单向函数的前方记录下在此过程中由携带证件向终端发出的回答 R_i 。在掌握了所有的回答时，对于该行骗者，就可作出一个伪携带证件，它包含着一个仅与对问题 Q_i 的回答 R_i 有关的表格，并在每当终端提出一个问题 Q_i 时对终端作出一个回答 R_i 。为了阻止这种诈骗，根据本发明考虑了两种解决方案。

根据本发明的第一个可被应用的解决方案，这是在表格中设置比可与终端相连接的携带证件数目多的非常大量的问题时才使用，在相应的问题一旦向携带证件提出后，就将表格中的整个一行抹去。企图截获对问题的回答的行骗者则不能使用这些问题因为任何一个相同的问题不会重新发送。对此应指出，终端最好有规律地以实时的方式经遥测传输线与主权机关的中心机构连接，以便重新存入或修改表格5。如果一个终端非常频繁地接收接口的请求，则可预先设置一个包括数千行的表格5。

根据第二个解决方案，如图3所示，在表格的每个问题中包括一个表格的指示符 I_t 。例如当问题是64位数串组成时，则

可将每个问题的开始十位预设成相同的并构成了表格的指示符。每个问题Qi因而具有It Pi形式，其中只有Pi是因问题而异的。因此网的每个终端包括一个有与其它终端不同的指示符的表格。此外，在携带证件的存储器11中存储了当该携带证件连接到终端时向其提出问题的每个表格的指示符，或最后的十个表格的指示符，或最常用的十个表格的指示符，并使一个计数器12与每个存储的指示符相联系，每当向携带证件传送了包含存储指示符的一个问题时该计数器12递增计数一次。此外，在携带证件的存储器13中存入一个阈值，并在每当向处理电路4发送一个问题时由一个比较器14将计数器12的值与阈值相比较。当计数器达到存储的阈值时，携带证件的处理电路4被截止以使得携带证件不再对相应的终端的问题作出答复。这样就阻止了行骗者获得对表格中所有问题的回答，并考虑到由终端发出的问题的随机性；就使由终端对伪证卡认证的危险减小到最低限度。在此情况下，表格的规模要比前例中的小得多，例如可预设一个一百行的表格及十个问题的阈值。在这种情况下，最好预设一个相当高的表格更换频率，其中包括它的指示符。

为了避免达到可引起携带证件电路截止的临界阈值，一个深谋远虑的行骗者可以制作一个混合了多个包含不同指示符的表格的新表格，其方式是在这些表格的每个表中每次取小于阈值的行数，以便获得对这样制作的新表格中问题的全部回答。根据表示在图4中的本发明这种方式的一个变型，考虑不仅在每个问题中而且在表格的一个存储器15中存储表格的指示符，并在向携带证件传送一个问题前，借助一个比较器16将问题的1X部分与表格的指

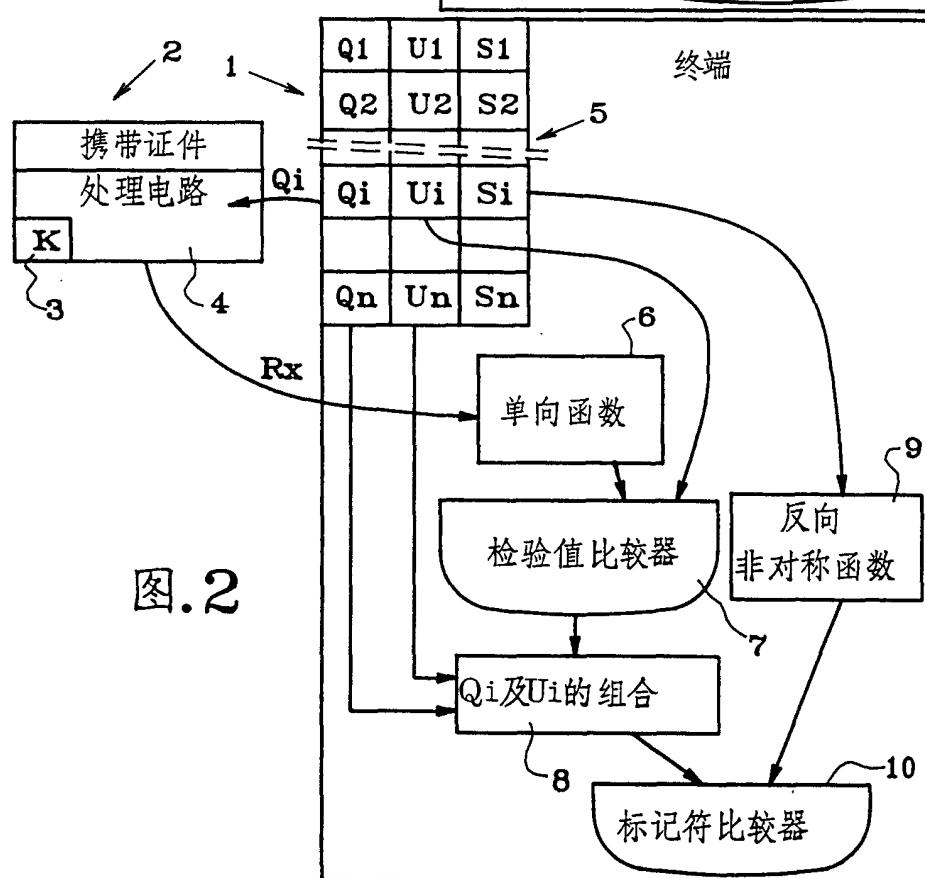
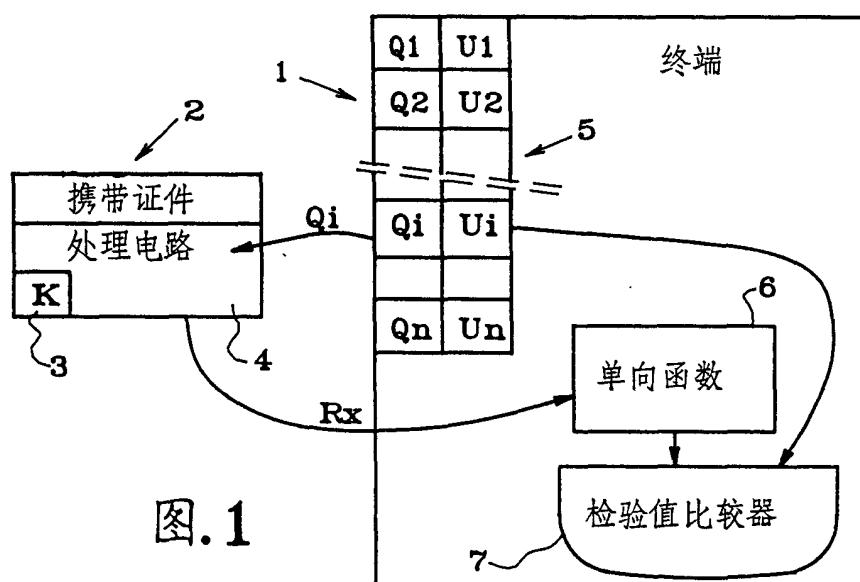
示符1t 相比较来保证该问题所包含的表格指示符有效地对应于所考虑的表格。如果发现了一个异常的标记符，终端则停止服务并可以在主权机关附近发出警报以便作出核查。

为了避免携带证件存储器的饱和，最好考虑当一个表格被修改时将携带证件的计数器复位到零。为此；例如在固定日期对不同终端的表格作出修改并在携带证件中存储将计数器复位至零的日期。这样每当一个携带证件与一个终端相连接时，就可以核查计数器被置零的最后日期是否在最新修改表格之前，如果是在这种将携带证件的计数器复位到零的情况下就同时消除了相应的指示符。

根据另一个实施变型，可以考虑设置有多个不同表格的终端，以便能对包含不同密码的携带证件认证，其中每个表格与一个密码相配合。这时每个携带证件包含一个应能对认证起作用的表格识别中间值以便所述的方法能够正确地进行。当连接时，携带证件向终端发送与它的密码相关的此种表格识别中间值，那时后面的认证操作就符合上述本发明的方法。

尽管本发明的涉及使用表格指示符的方式是联系本发明方法的基本形式描述的，但也可考虑使该方式联系具有多个表格的复杂形式来设置。

当然本发明并不局限于所描述的不同形式上，在不脱离如权利要求书所确定的本发明范围的情况下，对发明还可以作出各种实施的变型。



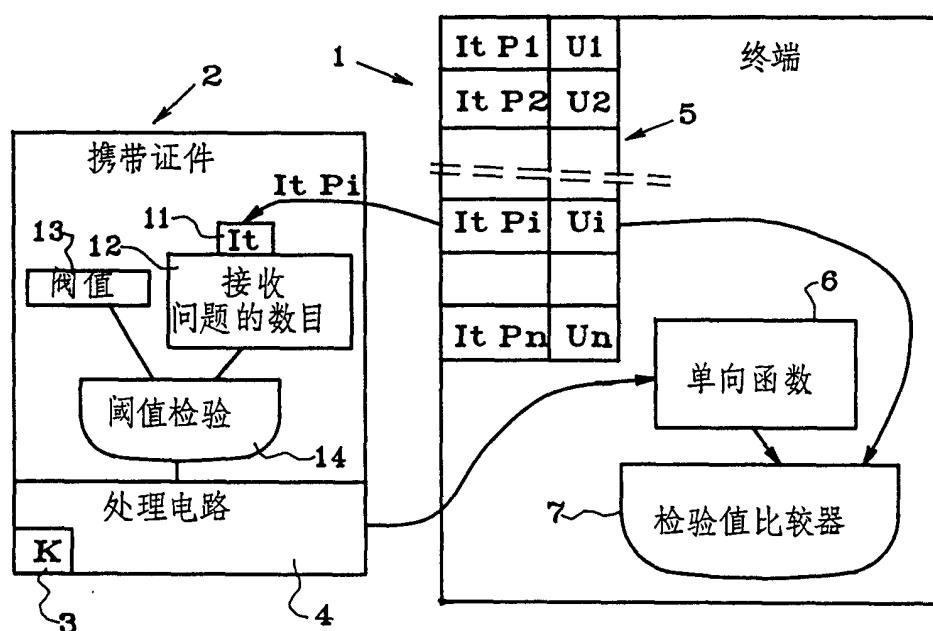


图.3

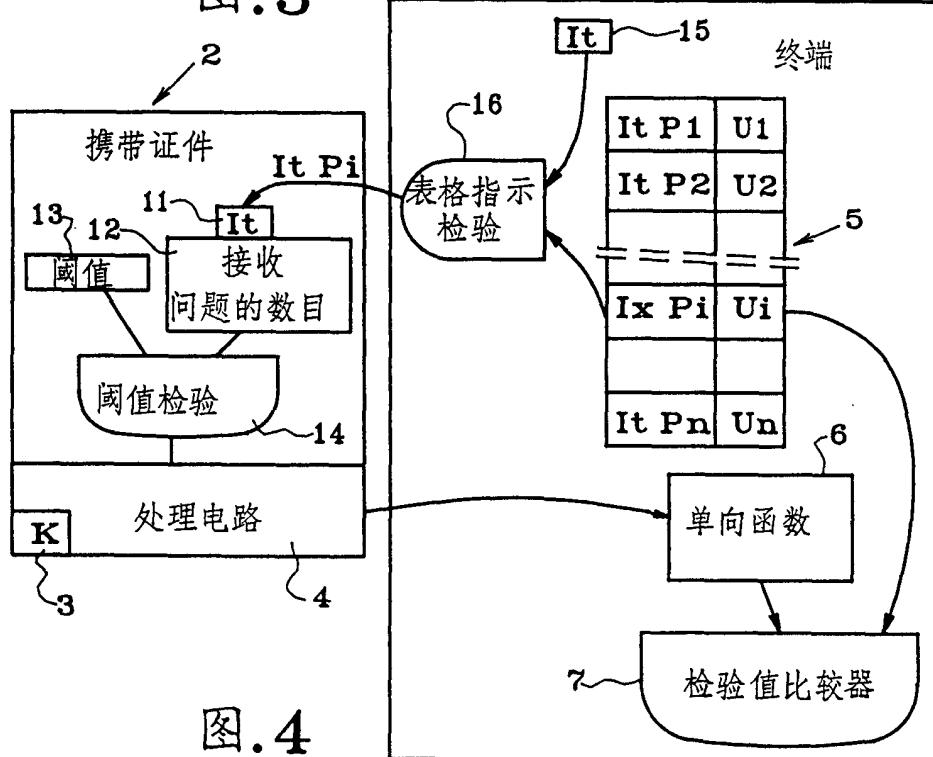


图.4