(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102024289 A
(43)申请公布日 2011.04.20

(21)申请号 200910195627.6

(22)申请日 2009.09.11

(71)申请人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路 36 号银联大厦

(72)发明人 孟宏文 何朔 鲁志军 庄晓

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 谭佐晞 李家麟

(51)Int.Cl.
G07F 7/08(2006.01)

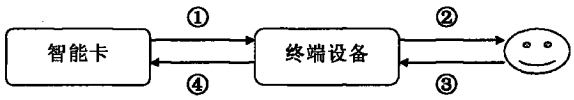
权利要求书 1 页 说明书 5 页 附图 1 页

(54)发明名称

一种安全获取智能卡密码的方法

(57)摘要

一种安全获取智能卡密码的方法，智能卡中设置有多个密码因素矩阵，每个密码因素矩阵中包括矩阵元素及其对应的元素值和索引，当持卡人在终端设备上使用智能卡时，智能卡输出密码因素矩阵给终端设备，持卡人根据密码的内容选择矩阵内的对应的矩阵元素，终端设备获取持卡人选择的矩阵元素的索引，并将该索引列表返回给智能卡，根据内部的对应关系找到元素值，得到持卡人输入的真实密码，因此，只有密码持有人和智能卡知道密码，屏蔽了包括终端读卡设备在内的第三方获取密码，有效地保护了密码在输入过程中的安全性。



CN 102024289 A

1. 一种安全获取智能卡密码的方法，其特征在于：智能卡中设有多个密码因素矩阵，每个密码因素矩阵中包括矩阵元素及其对应的元素值和索引，所述智能卡获取密码的方法包括下述步骤：

步骤 a、当持卡人在终端设备上使用智能卡时，智能卡输出密码因素矩阵给终端设备，终端设备根据密码因素矩阵的类型将该矩阵显示给持卡人；

步骤 b、持卡人看到显示的矩阵元素，并根据密码内容选择矩阵内的对应的矩阵元素；

步骤 c、终端设备获取持卡人选择的矩阵元素的索引，并将该索引列表返回给智能卡；

步骤 d、智能卡获取索引列表，根据内部的对应关系找到元素值，得到持卡人输入的真实密码。

2. 根据权利要求 1 所述的一种安全获取智能卡密码的方法，其特征在于：所述的矩阵元素是图片，或者是文本，或者是声音。

3. 根据权利要求 1 所述的一种安全获取智能卡密码的方法，其特征在于：所述密码因素矩阵，每个密码因素矩阵都有一个类型标识和一个矩阵 ID，每个矩阵有十个矩阵元素，每个矩阵元素都有对应的值。

4. 根据权利要求 1 所述的一种安全获取智能卡密码的方法，其特征在于：其中步骤 a 中还包括当持卡人使用智能卡时，智能卡选择多个密码因素矩阵中的一个作为输出到终端设备的密码因素矩阵。

5. 根据权利要求 1 所述的一种安全获取智能卡密码的方法，其特征在于：其中步骤 a 还包括当持卡人使用智能卡时，智能卡动态生成每个矩阵元素的索引，矩阵元素与其索引之间的对应关系在智能卡获取密码的过程中一直存在。

6. 根据权利要求 4 所述的一种安全获取智能卡密码的方法，其特征在于：所述智能卡选择一个密码因素矩阵是根据随机因素来确定的，随机因素包括终端设备的能力，终端的时间，终端随机数，卡随机数，卡内部的计数器，以及他们之间的任意组合。

7. 根据权利要求 5 所述的一种安全获取智能卡密码的方法，其特征在于：所述步骤 d 还包括，当终端设备向智能卡提交持卡人选择的矩阵元素索引后所述矩阵元素与索引之间的对应关系失效。

一种安全获取智能卡密码的方法

技术领域

[0001] 本发明涉及银行卡支付系统，尤其涉及银行卡支付系统中密码的安全获取方式。

背景技术

[0002] 银行卡 (Bank Card) 作为支付工具越来越普及，通常的银行卡支付系统，包括销售点终端 (Point Of Sale：POS)，终端管理系统 (Terminal Manage System：TMS)，密码键盘 (PIN PAD) 和硬件加密机 (Hardware and Security Module：HSM)。

[0003] 同时我国银行卡将逐步由磁条卡向 IC 卡即智能卡方向转变，智能卡容量大，防伪性能更强，是应对目前银行卡犯罪最有效的办法之一，事实上，目前在欧美等发达国家，磁条卡已经很少使用，人们的银行卡大多是智能卡。 在国内，早在 2005 年，就颁布了《中国金融集成电路 (IC) 卡规范》，是世界上第四部银行卡行业标准规范。 2006 年，央行又进一步完善了我国银行智能卡发展规划，鼓励商业银行发行基于电子钱包功能的智能卡。

[0004] 相比磁条卡，智能卡由于增加了读写保护和数据加密保护，在使用保护上采取个人密码、卡与读写器双向认证、芯片卡复制难度极高，具备很强的抗攻击能力，很难被复制和伪造。

[0005] 在现有技术中智能卡在获取密码的时候是由智能卡外部设备从持卡人那里直接获取密码，并将该密码直接传递给智能卡，如图 1 所示：

[0006] 持卡人通过密码输入设备直接输入密码，密码输入设备将密码传递给智能卡。可以看出，密码在传递到智能卡内时内容被密码输入设备所共享，造成信息泄露。

[0007] 要解决这个问题，必须做到密码只能由密码持有人和智能卡两者知道，屏蔽第三方；设计防止密码被窃取的机制。

发明内容

[0008] 本发明的目的在于：提供一种安全获取智能卡密码的方法，解决在密码输入过程中造成密码信息泄漏的问题。

[0009] 本发明提出了一种安全获取智能卡密码的方法，智能卡中含有多个密码因素矩阵，每个密码因素矩阵中包括矩阵元素及其对应的元素值和索引，所述智能卡获取密码的方法包括下述步骤：

[0010] 步骤 a、当持卡人在终端设备上使用智能卡时，智能卡吐出密码因素矩阵给终端设备，终端设备根据密码因素矩阵的类型将该矩阵显示给持卡人；

[0011] 步骤 b、持卡人看到显示的矩阵元素，并根据密码内容选择矩阵内的对应的矩阵元素；

[0012] 步骤 c、终端设备获取持卡人选择的矩阵元素的索引，并将该索引列表返回给智能卡；

[0013] 步骤 d、智能卡获取索引列表，根据内部的对应关系找到元素值，得到持卡人输入的真实密码。

[0014] 进一步地，所述的密码因素矩阵中矩阵元素是图片，也可以是文本，或者是声音及其他终端可以识别的方式，所述智能卡具有多个密码因素矩阵，每个密码因素矩阵都有一个类型标识和一个矩阵 ID，每个矩阵有十个矩阵元素，每个元素都有对应的值。

[0015] 进一步地步骤 a 中还包括当持卡人使用智能卡时，智能卡随机选择一个密码因素矩阵作为输出到终端设备的密码因素矩阵，所述智能卡随机选择一个密码因素矩阵是根据随机因素确定要使用的密码因素矩阵，随机因素包括终端设备的能力，终端的时间，终端随机数，卡随机数，卡内部的计数器，以及他们之间的任意组合。

[0016] 进一步地步骤 a 还包括当持卡人使用智能卡时，智能卡动态生成每个矩阵元素的索引，矩阵元素与其索引之间的对应关系在智能卡获取密码的过程中一直存在。 步骤 d 还包括当终端设备向智能卡提交持卡人选择的矩阵元素索引后所述矩阵元素与索引之间的对应关系失效。

[0017] 通过本发明的方法，有效地保证了密码输入过程的安全性。

附图说明

[0018] 图 1 为现有技术的智能卡密码获取过程；

[0019] 图 2 为本发明智能卡密码获取过程。

具体实施方式

[0020] 本提案提出一种安全输入智能卡所需密码 (PIN) 的方法，设计该方法的出发点是 PIN 是密码持有人和智能卡两者共享的私密信息，必须防止其他任何第三方获得该信息，包括密码输入设备在内也无法获取密码。

[0021] 本发明如图 2 所示，持卡人使用智能卡时，将智能卡插入终端设备，其获取密码的步骤如下：

[0022] 1、智能卡输出密码因素矩阵给终端设备，终端设备根据密码因素矩阵的类型将该矩阵显示给密码持有人；

[0023] 2、密码持有人看到或听到（人易感知，机器难感知）显示的矩阵元素，并根据密码内容选择矩阵内的对应矩阵元素；

[0024] 3、终端设备获取密码持有人选择的矩阵内的元素的索引，并将该索引列表返回给智能卡；

[0025] 4、智能卡获取索引列表，根据内部的对应关系找到真实的密码值，得到用户输入的真实密码。

[0026] 本发明在智能卡内部设计多个密码因素矩阵，针对终端设备的能力和其他随机因素共同确定某个时刻使用的密码因素矩阵，随机因素是指终端输入给卡片的时间、终端随机数、卡片随机数或卡片内部的计数器等，也可以是他们之间的任意组合；终端设备的能力是指 POS 用自带的键盘采用新的方法来输入密码，已不需要 PINPAD，它的能力主要是指显示器的显示能力，有的支持图形显示，有的只支持文本显示，还可能有的能力是声音输出能力（具备扬声器），或其他方式。

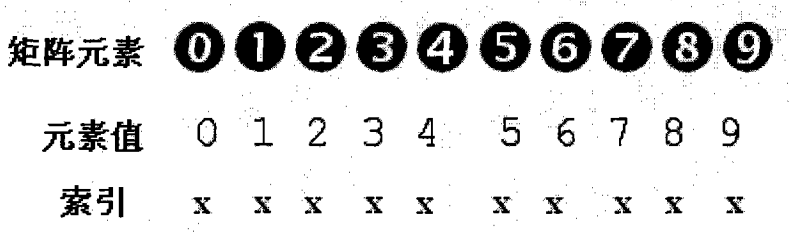
[0027] 然后将该矩阵输出给终端设备，该矩阵的标识由智能卡内部产生和解释，只有矩阵内元素的类型和索引是终端设备必须知道的。

[0028] 上述密码因数矩阵是由一组图片或字符串组成，其内容的含义由“人”去理解和感知，其本身并不能容易的被机器阅读或感知，典型的密码因数有图片类型和文本类型，这里以输入数字型的密码为例进行说明，每个矩阵都有一个类型标识和一个矩阵ID，每个矩阵有十个元素，每个元素都有对应的值。

[0029] 密码因数矩阵例 1：

[0030] 类型标识：01（代表图片），矩阵 ID ＝ 1

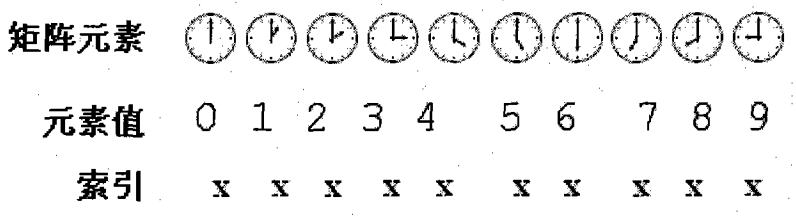
[0031]



[0032] 密码因数矩阵例 2：

[0033] 类型标识：01（代表图片），矩阵 ID ＝ 2

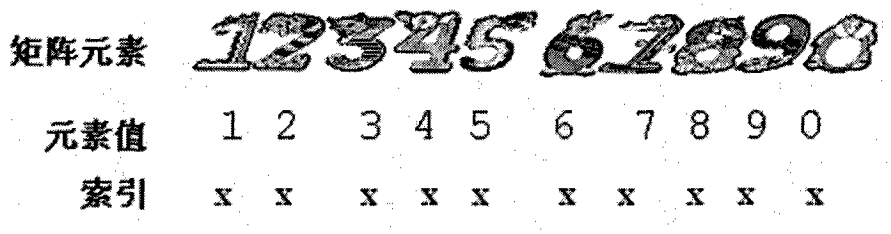
[0034]



[0035] 密码因数矩阵例 3：

[0036] 类型标识：01（代表图片），矩阵 ID ＝ 3

[0037]



[0038] 密码因数矩阵例 4：

[0039] 类型标识：02（代表文本），矩阵 ID ＝ 4

[0040]

矩阵元素	元素值	索引
嘴张开像什么?	0	x
棍子代表?	1	x
1＋1的值	2	x
4-1的值	3	x
1984的最后一个数字	4	x
一把手的手指个数	5	x
3+3的值	6	x
中文发音为“吃”的数字	7	x
代表“发”的数字	8	x
中文发音为“酒”的数字	9	x

[0041] 矩阵内的每个元素在智能卡内都是分别存储的，当终端设备请求矩阵信息时，由智能卡内部动态生产一个矩阵元素与其索引之间的临时的对应关系，并将该临时的对应关系作为索引连同矩阵元素一起返给终端设备，即动态生成每个矩阵元素的索引。 持卡人选择矩阵元素后，所有持卡人选择的矩阵元素对应的索引将被返回给智能卡。 当外部请求输入密码时，其可能带入的参数有：终端的能力、终端的时间和终端随机数，卡片根据终端的能力确认终端具备何种输出能力，随即选中合适的矩阵，然后根据终端的时间和终端随机数及卡内的随机数根据一定的算法计算出一个“种子”，用该种子再用单向函数（如：SHA1、 MD5、 MAC 等）计算出一个数，作为第一个矩阵元素的索引，然后用该索引作为计算下一个索引的输入，如此循环，计算出所有的索引。 另一个简单的方法可以是将种子作为索引的起点、中点或终点，进行简单计算得出所有的索引，假如种子是 10，假设采用等差递增序列：

[0042] 种子做起点：递增为 2，则得到的索引：10，12，14，16，18，20，22，24，26，28；

[0043] 种子做中点：递增为 2，则得到的索引：0，2，4，6，8，10，12，14，16，18；

[0044] 种子做终点：递增为 2，则得到的索引：-10， -8， -4， -2，0，2，4，6，8，10。

[0045] 当终端设备提交用户选择的矩阵索引后该对应关系失效，当然，失效的条件还可能有：

[0046] 终端设备重新请求矩阵信息重新启动密钥输入的过程；

[0047] 终端设备选择了另外一个智能卡上的应用；

[0048] 智能卡掉电；

[0049] 其他定义的失效条件。

[0050] 通过本发明的方法，有效地保证了密码输入过程是安全的，因为密码没有直接出现，要盗用密码的唯一办法是蛮力攻击，但因为我们有三道关口，其攻击的难度很大。 关口 1：密码矩阵，根据终端能力选择；关口 2：密码索引，随机生成；关口 3：矩阵元素，人宜懂，机器难以识别。

[0051] 智能卡需要密码的时候，由终端设备从智能卡上读取一个密码要素矩阵，该矩

阵的内容容易为人所识别，例如密钥要素可能是图片，也可能是一个简单的提问，这些都容易被人所识别，但不容易机器设别，密码获取时终端设备记录密码持有人选择（或点击）矩阵的索引标识，并将索引标识返回智能卡，由于只有智能卡知道每张图片对应的密码值（可以是数字或字母），这样就屏蔽了密码输入设备获得密码的可能，保证了密码的私密性。

[0052] 可见，本发明有效的保障了密码的私密性，密码在传递过程中没有出现，所以避免了泄密的可能；密码输入设备尽管参与密码的“输入”过程，但被有效屏蔽；能够适应不同的密码输入设备的能力。

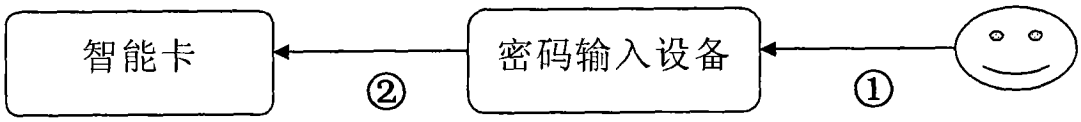


图 1

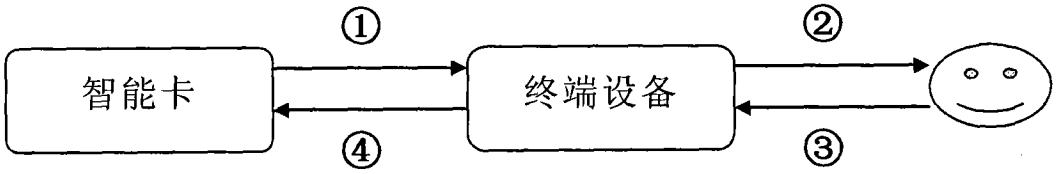


图 2