[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 96198809.6

[43]公开日 1998年12月30日

[11]公开号 CN 1203681A

[22]申请日 96.11.14

[30]优先权

[32]95.12.8 [33]NL[31]1001863

[86]国际申请 PCT/EP96/05027 96.11.14

[87]国际公布 WO97/22091 英 97.6.19

[85]进入国家阶段日期 98.6.5

[71]申请人 康克里克PTT荷兰公司

地址 荷兰海牙

[72]发明人 杰利·威森伯格 约翰尼斯·布雷勒
弗兰克·马勒 马丁·K·德兰格
艾伯塔斯·费肯
亨德里卡斯·J·W·M·范德佩维特

[74]专利代理机构 柳沈知识产权律师事务所

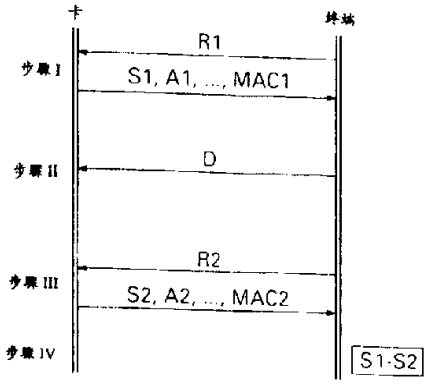
代理人 马莹

权利要求书 2 页 说明书 7 页 附图页数 3 页

[54]发明名称 保护地记入电子付款工具借方的方法

[57]摘要

本发明涉及一种用于保护交易的方法，该方法用于一个所谓的智能卡（11）和诸如现金出纳机的一个终端（12）。为防止智能卡与几台终端同时进行交易，本发明提供了一个在智能卡（11）与终端（12）交换数据时使用的鉴别值（A），唯一地确定交易的后续步骤。



权　利　要　求　书

1. 采用付款工具（ 11 ）及付款台（ 12 ）来进行交易的方法，所述方法包括重复执行如下询问步骤（ I， III ）: 付款台（ 12)询问付款工具（ 11 ），并接受付款工具的回应数据（如 S1， S2 ），付款工具的数据包括由预定处理过程（ F)生成的鉴别码（ MAC1， MAC2)和后续鉴别码(如 MAC2)，后者通过付款工具（ 11 ）和付款台共同生成的鉴别值（如 A2 ）与同一交易的前鉴别码（ MAC1 ）相联系。

2. 如权利要求 1 所述的方法，其中，鉴别值（如 A1 ）在每一询问步骤中（如 I ）均被替换。

3. 如权利要求 1 或 2 所述的方法，其中，处理过程（ F ）包含一关键码（ K ）。

4. 如权利要求 1 或 2 或 3 所述的方法，其中，处理过程（ F ）包含一个由付款台（ 12 ）生成的随机数（如 R2 ）和一个付款工具余额（如 S2 ）。

5. 采用一付款台（ 12 ）来有保护地记入电子付款工具（ 11 ）借方的方法，所述方法包括:

- 第一步（ I ），其中:

- 付款台（ 12 ）传送第一随机数（ R1 ）到付款工具（ 11 ）。

- 付款工具（ 11)回应所述第一随机数（ R1), 传送第一鉴别码（ MAC1 ）至付款台（ 12 ），其中第一鉴别码（ MAC1)至少要根据第一随机数（ R1 ）和第一鉴别值（ A1 ）来确定，以及

- 付款台（ 12 ）检查第一鉴别码（ MAC1 ）;

- 可选的第二步（ II ），其中:

- 付款台传送一记入借方命令（ D ）至付款工具（ 11 ），付款工具的余额（ S1 ）根据记入借方命令减少；以及

- 第三步（ III ），其中:

- 付款台（ 12 ）传送第二随机数（ R2 ）到付款工具（ 11 ）。

- 付款工具（ 11)回应所述第二随机数（ R2), 传送第二鉴别码（ MAC1 ）至付款台（ 12 ），其中第二鉴别码（ MAC2)至少要根据第二随机数（ R2 ）和第二鉴别值（ A2 ）来确定，第二鉴别值（ A2 ）由第一鉴别值（ A1 ）推出。以及

- 付款台（ 12 ）从第一鉴别值（ A1 ）推出第二鉴别值（ A2 ），并检查第二鉴别码（ MAC2 ）。

6. 如权利要求 5 所述方法，其中，第一、第二鉴别值（ A1， A2 ）相同。

7. 如权利要求 5 所述方法，其中，第一、第二鉴别值（ A1， A2 ）包括连续计数器值。

8. 如权利要求 5 所述方法，其中，鉴别值（如 A2 ）每次根据随机数（如 R2 ）和前鉴别值（ A1 ）来生成。

9. 如前述权利要求中任一项所述方法，其中，鉴别码（如 MAC2 ）根据关键码（ K ）和识别码来确定。

10. 如前述权利要求中任一项所述方法，其中，鉴别码（如 MAC1 ）由密码函数（ F ）来帮助确定。

11. 如前述权利要求中任一项所述方法，其中，在第一与第三步中（ I，III ），付款工具（ 11 ）传送一个余额（如 S1 ）给付款台（ 12 ）。

12. 如前述权利要求中任一项所述方法，其中，在第一与第三步中（ I，III ），付款工具（ 11 ）传送当前鉴别值（如 A1 ）给付款台（ 12 ）。

13. 如前述权利要求中任一项所述方法，其中，第三步（ III ）可重复多次。

14. 如前述权利要求中任一项所述方法，还包括第四步（ IV ），其中第一步与第三步中余额的差值（ S1 - S2 ）被记到付款台（ 12 ）中。

15. 如前述权利要求中任一项所述方法，其中，第一随机数（ R1 ）等于第二随机数（ R2 ）。

16. 如前述权利要求中任一项所述方法，其中，付款台（ 12 ）包括一个有保护地记录数据模块。

17. 应用如前述权利要求中任一项所述方法完成的金融交易。

18. 电子付款工具（ 11 ），包括一个含处理器（ 101 ），存储器（ 102 ），及输入/输出回路（ 103 ）的集成电路，用于实现权利要求 1 至 16 中所述方法。

19. 付款台（ 12 ），用于应用权利要求 1 至 16 中所述方法。

说　明　书

保护地记入电子付款工具借方的方法

本发明涉及一种记入诸如含集成电路的电子付款卡（ IC 卡）的电子付款工具借方的方法。特别地，但不是专门地，本发明涉及一种保护地记入应用于诸如电话亭的预付电子付款卡（“预付卡”）借方的方法。在本文的正文中，术语“付款工具”不特指具体的付款工具的形式和类型。因此，一种付款工具可以是可记帐的付款卡，也可以是非卡片形式的电子付款工具。

近年来，电子付款工具普遍使用，不仅用于公用电话付款，也用于其他一些目的的付款。由于这种付款工具通常包括一个代表钱数的（贷方）余额(balance)，因此需要在这种付款工具和以保护模式（付款协议）运行的付款台（如设计成电子付款的电话或电子收银机）之间交换数据。 此处需要确保，如，记入付款工具借方的某金额（钱数或核算单位）对应于记入其他某处贷方的金额（钱数或核算单位）：顾客付出的金额必须对应于供应商收到的金额。记入贷方的金额可以存放到如付款台的保护模块中。

如欧洲专利申请 EP 0,637,004 中所述的现有技术的付款方法,包括: 第一步，付款台检索(retrieve)付款工具的余额；第二步，付款工具的余额降低（记入付款工具借方）；第三步，付款台再次检索付款工具的余额。根据第一步与第三步中余额的差值，记入付款台贷方的金额就可以确定了。第二步可以多次重复，并可能与第三步一起重复多次。

为防止欺诈，这种方法中的第一步采用一个付款台生成的随机数，并，作为检索余额代码的一部分传送到付款工具中。根据上述随机数，付款工具的第一回应是生成一个鉴别码，它包括经处理（如加密）的随机数、余额，和其他数据，每次交易采用不同的随机数，就可以防止通过回应来模仿交易。之后，第三步采用第二个随机数，它也由付款台产生，并传送给付款工具。根据第二随机数，付款工具的第二回应是产生第二个新的鉴别码，它包括经处理的第二个随机数、新余额，以及其他数据。根据两次传送的余额差值，付款台（或可能是付款台的保护模块）就可以确定付款台应记入贷方的金额。

只要付款工具只同一个付款台（或保护模块）联通，上述公知方法一般是非常不易被欺骗的。然而上述方法的不足在于，第一与第二次鉴别码是独立的。若第二或第三个付款台（保护模块）与付款工具联通，就可能因为上述独立性，使第一步与第二、三步分割开来。结果是表面上交易完成，但发现被记入付款工具借方的金额与记入了这几台付款台（保护模块）的贷方的总额不同。可以理解这种情况是不希望发生的。

US 专利 US 5,495,098 以及相应的欧洲专利申请 EP 0,621,570 揭示了一种方法，采用付款台安全模块身份识别，以确保只在卡和一个终端之间进行数据交换。安全模块、付款台和卡之间的数据交换保护比较复杂，需要大量密码计算。

其他现有技术如欧洲专利申请 EP 0,223,213 和 EP 0,570,924 也提到了一些，但都没有提供解决上述问题的方案。

本发明的目的是消除现有技术的上述缺陷，以及其他一些缺陷，并提供一种方法，它对记入借方交易提供更大程度的保护。特别的，本发明的目标是提供一种方法，确保交易期间只在付款工具与一台付款台或保护模块间联通。更特别的，本发明的目标是提供一种方法，确保交易时付款工具余额中降低的金额对应于仅一台付款台或保护模块的余额中增加的金额。

因此，本发明提供一种采用付款工具和付款台进行交易的方法，此方法包括执行一个反复询问的步骤：付款台询问付款工具，并接受付款工具回应的数据。付款工具数据包括一个由预定处理生成的鉴别码，一个后续鉴别码，它通过付款工具与付款台共同产生的鉴别值与同次交易的前序鉴别码相关联。鉴别值与鉴别码关联，就可以区分初始交易的鉴别码和干扰交易的鉴别码。更适宜的，每次询问步骤中的鉴别码都变更，从而增加了安全性。

更具体地，本发明提供了一种有保护地采用付款台记入电子付款工具借方的方法，该方法包括：

- 第一步，其中：
- 付款台传送第一随机数到付款工具，
- 付款工具响应上述第一随机数而传送第一鉴别码到付款台。其中第一鉴别码的确定至少要根据第一随机数和第一鉴别值，及
- 付款台检查第一鉴别码；
- 可选的第二步，其中：

- 付款台传送一个记入借方命令给付款工具，根据记入借方命令，付款工具的余额降低；及

- 第三步，其中:

- 付款台传送第二随机数给付款工具，

- 付款工具响应上述第二随机数而传送第二鉴别码到付款台，其中第二鉴别码的确定至少要根据第二随机数和第二鉴别值，第二鉴别值由第一鉴别值推出，及

- 付款台从第一鉴别值推出第二鉴别值，并检查第二鉴别码。

根据相互关联的鉴别值及其他数据形成的鉴别码，就有可能检查第二鉴别码（第三步中）是否与第一鉴别码相关（第一步中）。现在通过每次产生一个新的鉴别值，由此确定一个鉴别码，就可以区分连续鉴别码，从而区分与不同交易相关的鉴别码。如果，每次执行第一与第三步骤时，产生一个特别的鉴别值，它能明确地确定第二鉴别码与与第一鉴别码的对应关系。因此，也就可以确定在某次交易中是否第二鉴别码已经被发出。

通常，鉴别值由付款工具自动产生。这就不太会受外界的影响，可以防止欺诈。鉴别值可以以各种方式生成，如通过随机数发生器或计数器。

交易的第一和第二鉴别值的相互关系可以是相同值或相互依赖值，例如计数器的序列值。同样，第一鉴别值可能是个随机数，第二鉴别值可能是在它上加一个特定数来生成。基本上，每对鉴别值的相互关系必须可以被确切检查。

本发明进一步的目标是提供应用本方法的电子付款工具和付款台。

下面将参照附图对本发明进行更详细的说明，其中:

图 1 是应用本发明的付款系统的示意图;

图 2 是应用本发明的方法的示意图;

图 3 是产生图 2 方法采用的鉴别码的示意图;

图 4 是本发明采用的付款工具的集成电路示意图。

以图 1 中所示用于电子付款的系统 10 为例，它包括一电子付款工具，如称为芯片卡(chip card)或智能卡的 11，一个付款台 12，第一付款场所 13，和第二付款场所 14。付款台（终端） 12 在图 1 中所示的是一台收银机，但也包括如（公用）电话。付款场所 13 与 14 在图 1 中均以银行来表示，但也可以是其它在自己设备（计算机）上处理付款的场所。实际中，付款场所 13

和 14 可能是一个付款场所。如例中所示，付款工具 11 包括基板和一个含触点 15 的集成电路，此集成电路用于处理（付款）交易。付款工具还可包括一个电子钱夹。

交易时，在付款工具 11 和付款台 12 间交换付款数据 PD1 。付款工具 11 与付款场所 13 相联系，付款台 23 与付款场所 14 相联系。交易后，付款场所 13 与 14 间通过交换付款数据 PD2 来结帐， PD2 由付款数据 PD1 推出。交易中付款台 12 与付款场所 14 一般不进行联通（成为离线系统）。因此交易必须在受控条件下才能发生，以确保系统不被滥用。这种滥用可能会导致，如增加付款工具 11 的余额，而与付款场所 13 中副本帐户的余额变化不匹配等情况。

图 2 表明了用“卡”（图 1 中 11 ）表示的付款工具（的集成电路）与用“终端”（图 1 中 12 ）表示的付款台（的保护模块）之间数据的交换情况，发生顺序用一个在另一个之下示出。

在用 I 表示的第一步中，终端（付款台）生成第一随机数 R1 并将此数传给卡（付款工具）（子步骤 Ia ）。实际上，随机数 R1 可以是用来检索鉴别码的代码的一部分。根据本发明，卡和终端通过计数器递增，启动随机数发生器，或两者都进行，来生成第一鉴别码 A1 。根据随机数 R1 ，第一鉴别码 A1 和包括付款工具的余额 S1 的其他数据，卡生成一个鉴别码 MAC1=F(R1,A1,S1...)，其中 F 可以是一个已知的密码函数（子步骤 Ib)。卡数据 S1 和 A1 以及鉴别码 MAC1 被送到终端（子步骤 Ic ）。终端根据 R1 ，S1 ， A1 以及其他数据检查鉴别码，若检查结果正确，记录余额 S1 。

需要注意的是，值 A1 传送到终端在本发明中不是必需的，但它提供了对欺诈的额外防护。

在用 II 表示的第二步中，终端生成一个记入借方命令 D ，其中包括记入付款工具借方的金额（钱数）。记入借方命令 D 被传到卡中，之后，付款工具的余额 S1 由记入借方的金额降低至 S2 。第二步可以重复多次。

在用 III 表示的第三步中，终端生成第二随机数 R2 ，并将它传到卡上（子步骤 IIIa ）。卡生成第二鉴别值 A2 。根据第二随机数 R2 、第二鉴别值 A2 及包括新的卡余额 S2 的其他数据，卡生成一个鉴别码 MAC2=F （ R2 ，S2.....），其中 F 可以是已知的密码函数（子步骤 IIIb ）。卡余额 S2 及鉴别值 A2 以及鉴别码 MAC1 被传到终端（子步骤 IIIc ）。第三步的运行与第一

步完全类似。

终端通过重新生成鉴别码并比较随机数 R2 来检查接收到的鉴别码 MAC2。终端还检查接受到的第二鉴别值 A2 是否等于终端中相应生成的值。若鉴别值 A2 不相等，交易中断，终端的余额不被修改。

若检查鉴别码 MAC2 正确，终端记录余额 S2。之后进行译码处理，如运行函数 F 的反函数，而不是重新生成鉴别码 MAC1 和 MAC2。

在用 IV 表示的第四步中，余额 S1 和 S2 的差值被确定并记录到终端上。在这一连接中，此差值可以被独立存储或加到已有值（终端余额）上以后再处理。上述第四步以及随后的可能步骤对本发明而言也不是必须的。一鉴别或确认步骤可位于图 2 所示的步骤之前；然而，这一步骤对于本发明不是必须的。

在前述示意图中，随机数 R1 和 R2 不一样，但随机数 R1 和 R2 可以相同（ R1=R2=R ），不过在步骤 III 中，也需要检查是否鉴别码 MAC2 使用的是同一随机数 R(= R1)。

需要注意的是，严格说来，数 R1 与 R2 一样不必是随机数，它用于确切地确定作为对 R1 的回应（“应答”）的鉴别码 MAC1，它只在 R1 不能被卡识别时才是必须的。

根据现有技术的方法，鉴别码 MAC1 和 MAC2 一般是独立的。这就是说，若随机数 R1 和 R2 不同， MAC1 码与 MAC2 码之间没有直接或间接的关系。基于这种独立性，一般无法保证步骤 I 和 III 是在同一卡和同一终端之间完成的。

然而根据本发明，确定第二鉴别码时所采用的鉴别值直接与确认第一鉴别码时所用的鉴别值有关。因此该交易的两个鉴别码之间建立起一种联系，这种联系是相当简单明了的（如 A2=A1+1 ），并允许简单的检查。

如果卡在已经输出了第一鉴别码 MAC1 至第一终端后，从第二终端接受了一个（第一）随机数 R1’，卡将输出一个鉴别码 MAC2。若随后第一终端在输出一个记入借方命令后，再次检索到一个鉴别码，卡再输出一个基于鉴别值 A3 以及其他数据的鉴别码 MAC3，终端将发现鉴别码 MAC1 和 MAC3 无关，就不会使用包含在鉴别码 MAC3 中的余额值 S3。同样地，被第二终端检索到的鉴别码 MAC4 提供了一个非有效的鉴别，所以提供一个非有效的余额值。在此方式下，修改后的余额值被传送到几台终端上的情况就

被有效地防止了。

鉴别值适宜用连续数，如计数位来形成。然而也可以用一个每隔一次（第二次产生鉴别值时）加一的计数器，这样每次两个连续鉴别值相等。需要注意的是付款工具可以区分第一步与第三步，但没有这个必要。

本发明中鉴别值之间的上述依赖性保证了应用本发明方法的交易中的所有步骤都只在同一卡与同一终端间进行。

图 3 示意鉴别码 MAC （“信息鉴别代码”），如图 2 中的 MAC1 和 MAC2，是怎样生成的。几个参数被输入到体现以"F"表示的函数的处理工具 20 中，函数 F 可能是一个密码函数（如众所周知的 DES 函数）或称为“散列”函数，这两者在技术上都是公知的。函数 F 也可以是一个相对简单的组合函数。在这种情况下处理工具 20 可包括一个带选择反馈的移位寄存器。输入到处理工具 20 中并因此输入到 F 中的参数，以图 3 为例，为随机数 R，卡余额 S，鉴别值 A，一关键码 K 及初始化向量（初始值）Q。随机值 R 对应如分别在第一步与第三步被传送到卡中的 R1 和 R2；卡余额 S 对应如被存放在卡中的 S1 和 S2。关键码 K 可能是一个为某一卡或某一些卡专用的密码。一个关键码识别器可以在图 2 步骤 I 前的鉴别或确认步骤时与终端交换。

初始化向量 Q 用于初始化函数 F，可以只有一个固定值，如 0。也可以取决于交易前续步骤完成后函数 F 的剩余数（最终状态）。更适宜地，向量 Q 在新交易开始时重置。

鉴别值 A 在例中是由计数器 21 生成。计数器最好在每一询问步骤时（如第一步与第三步）递增，即回应随机数 R 而生成鉴别代码（ MAC ）时。这使得每次用于鉴别码的鉴别值 A 不同。因为递增（此情况 + 1，但 + 2，+ 10 也是可以的）可以预定，因此终端能确认鉴别码。更适宜的，鉴别值能被传送到终端，并被终端确认。新交易开始时计数器 21 重置。

在图 3 的例中，鉴别值 A 由计数器产生，可以替换地，计数器 21 被一随机数发生器替代，它为交易的每一询问步骤（如第一步或第三步）生成一个新的鉴别值 A。在这种情况下前一步骤中的鉴别值必须被用作随机数发生器的初始化向量（“种子”），以便保持鉴别值间的相互依赖性及再现能力。

需要明白的是图 3 的设计适用于卡与终端二者，终端也生成鉴别值 A1,A2.....及鉴别代码 MAC1,MAC2.....，并将它们与相应的从卡中接收到的鉴别码及鉴别值相比较。余额 （如 S2 ）只有在生成的及接收的鉴别码和

鉴别值相等时才会被终端接收。

根据图 4 将进一步解释本发明的方法怎样应用于付款卡。

图 4 显示了一个电路 100，它包含一个控制单元 101，存储器 102 及一个输入/输出单元 103，它们相互连在一起。控制单元可由如微处理器或微控制器组成。存储器 102 可以包括一个 RAM 及/或 ROM 存储器。存储器 102 最好包括一个可擦写 ROM 存储器（ EEPROM ）。

根据本发明，电路 100 还包括一个附加存储器 105，用于存储鉴别值，如图 4 所示。上述存储器 105 可以是一个独立单元，但也可以是存储器 102 的一部分，如电存储器 102 的一些存储位组成。存储器 105 最好由一个计数器电路组成。 也可用图 3 中所示的独立计数器电路。

在优选实施例中，连续鉴别值由连续计数器位形成。用于形成鉴别代码 MAC1 的第一鉴别值 A1 对应于计数器的一个位置，存放在存储器 105 中。在第二步之后（也见图 2 ），计数器位加一。初始计数器位可能是随机的，但也可以重置为某预定值，如 0 。

生成鉴别值是自动进行的，即不受外界的影响。因此，防欺诈的能力进一步增强。

要明白的是，与其每次计数器位加一，不如每次减一。同样计数器位也可以增或减一位以上，如 2 或 4 。也可以以如下方式构造回路 100： 鉴别值在每次交易期间不修改，只是在进行不同交易时才修改。在此情况下，付款台也要相应改动。

应用于本发明的付款台包括用于与付款工具联通的设备（如读卡机），用于完成鉴别的设备（如处理器）及用于记录余额值的设备（如半导体存储器）。付款台以如下方式构造: 不成功的鉴别导致新余额值不能被记录。根据本发明，鉴别还包括鉴别值。本发明中的各步骤可以用设备（特殊电路，如 ASIC ）和软件（适当的处理器程序）来完成。

本领域的技术人员会明白: 本发明不限于所示的实施例，在不偏离本发明的范围的前提下，可以进行修改和补充。因此，虽然本发明的原理是基于记入付款工具借方的情况而描述，但上述原理也能适用于记入付款工具贷方的情况。

说 明 书 附 图

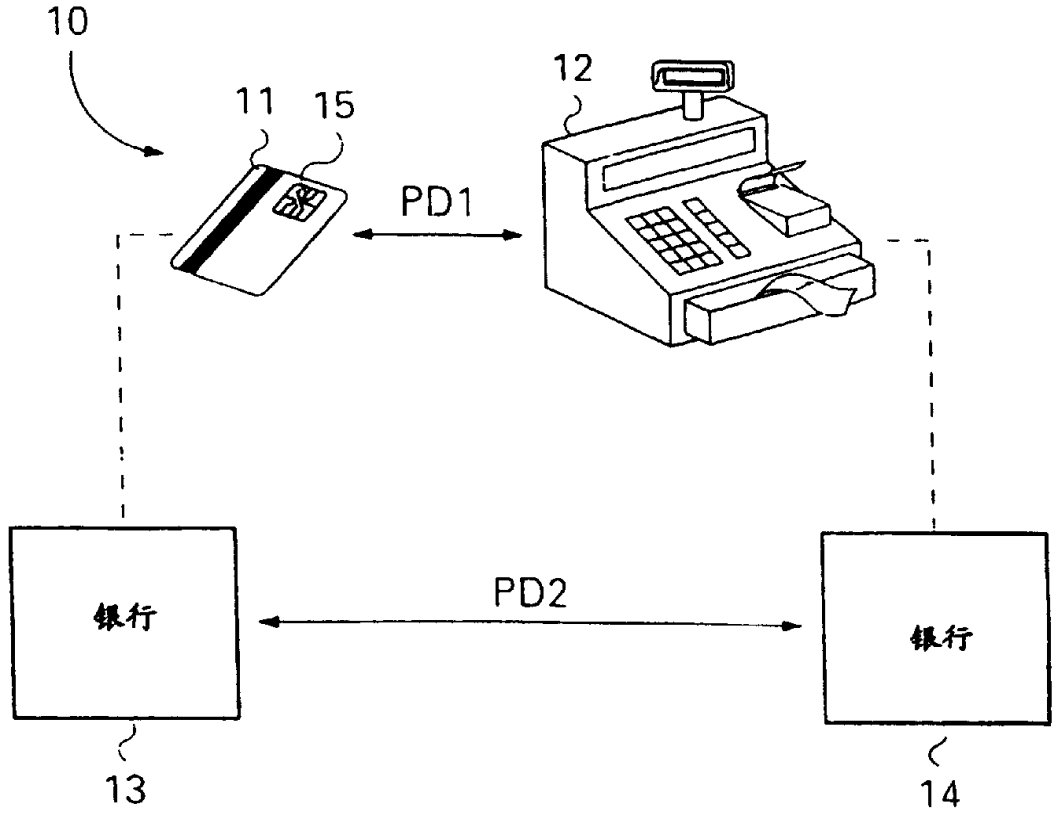


图 1

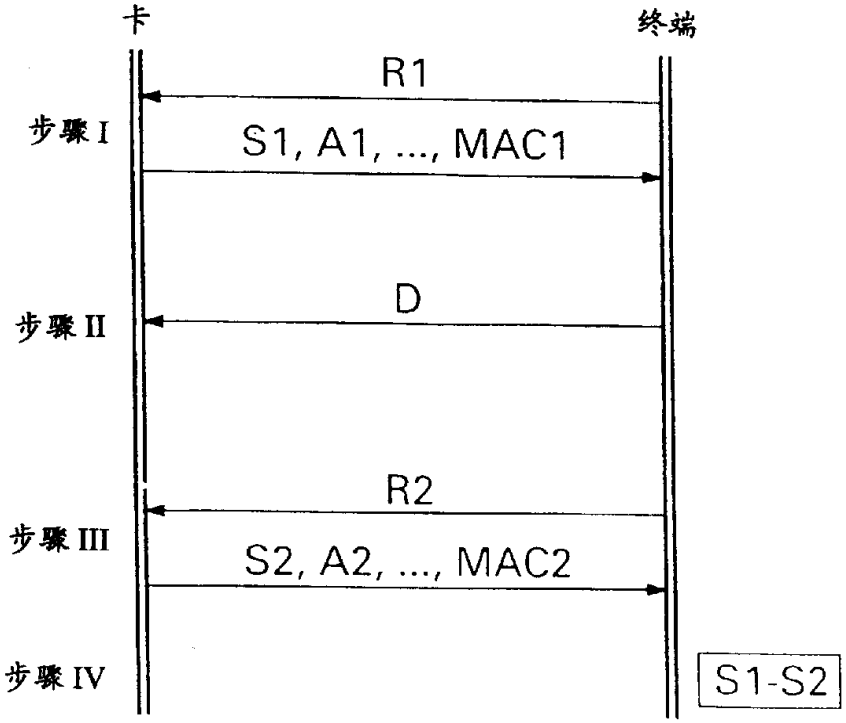

卡
终端
R1
步骤 I
S1, A1, ..., MAC1
D
步骤 II
R2
步骤 III
S2, A2, ..., MAC2
步骤 IV
S1-S2

图 2

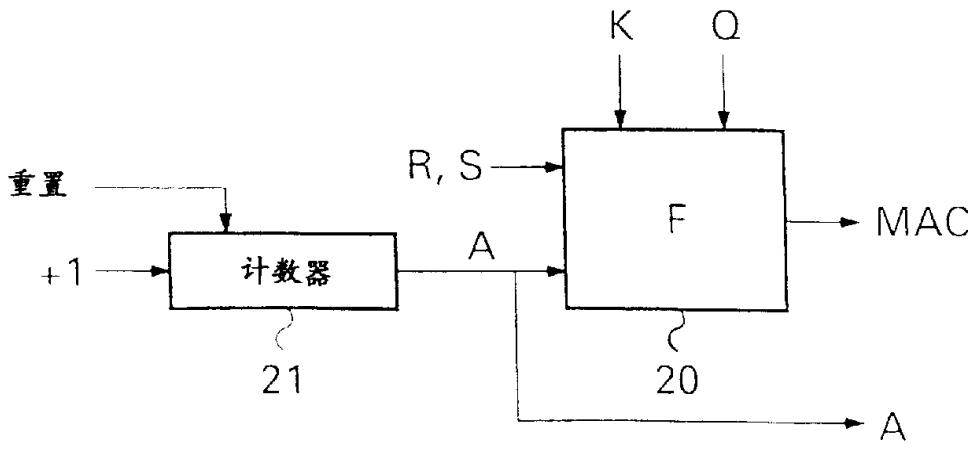

K
Q
R, S
重置
F
MAC
+1
计数器
A
21
20
A

图 3

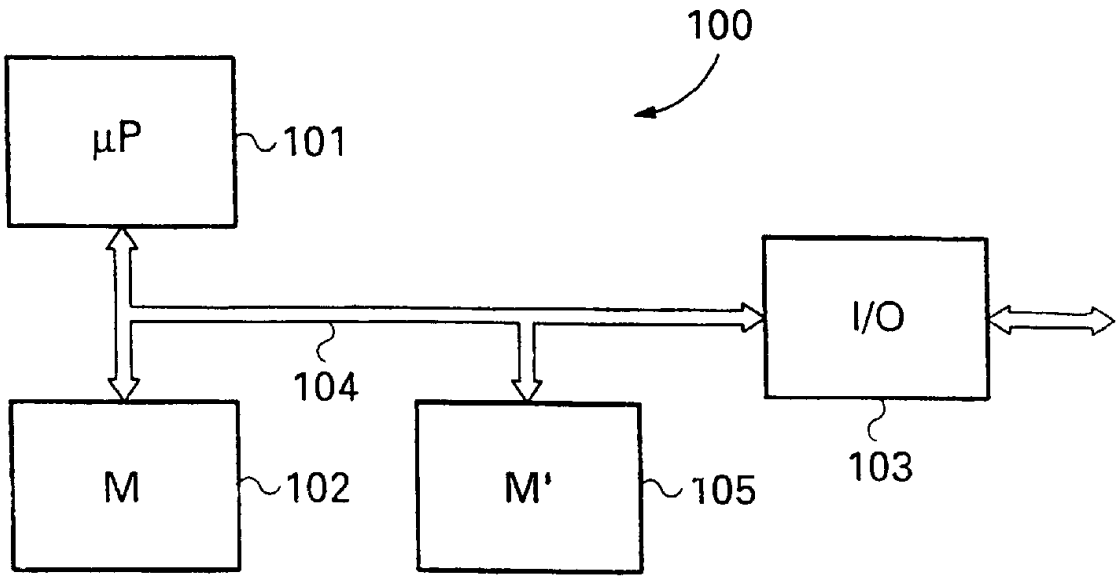


图 4