

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 17/60

[12] 发明专利说明书

[21] ZL 专利号 94192780.6

[45] 授权公告日 2002 年 12 月 18 日

[11] 授权公告号 CN 1096648C

[22] 申请日 1994.6.2 [21] 申请号 94192780.6

[30] 优先权

[32] 1993.6.2 [33] US [31] 08/071283

[86] 国际申请 PCT/US94/06031 1994.6.2

[87] 国际公布 WO94/28498 英 1994.12.8

[85] 进入国家阶段日期 1996.1.15

[73] 专利权人 惠普公司

地址 美国科罗拉多州

[72] 发明人 L·S·中村 A·B·罗伯斯

J·F·希斯

审查员 葛宝成

[74] 专利代理机构 中国专利代理(香港)有限公司

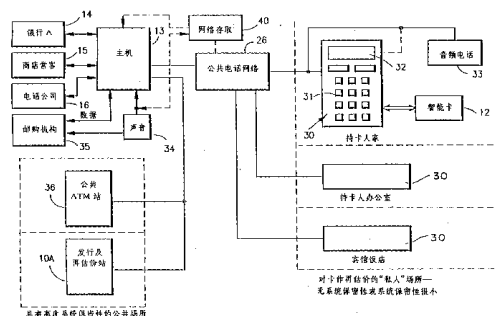
代理人 王 勇 张志醒

权利要求书 5 页 说明书 21 页 附图 8 页

[54] 发明名称 对存贮在 IC 卡中的标记值作再估价
的系统和方法

[57] 摘要

通过与远程设置上操作上兼容的终端进行联机交易对话,在私人场所执行一项包括改变存贮在持卡人的 IC 卡中的标记值的交易的一个终端。该私人终端建立与此 IC 卡和此远程终端的数据链路,并经由这些数据链路在相互之间传送保密的认证与交易信息,信息的保密性依赖于 IC 卡和远程终端。



ISSN 1008-4274

1. 在私人场所通过与远程位置操作上兼容的终端进行联机交易对话, 改变存贮在持卡人的 IC 卡中的标记值的一种方法,

所述 IC 卡具有一个微控制器和相关的

微控制器程序存贮器, 标记值数据和卡保密数据的保密保护存贮单元, 一个数据通讯接口, 以及存贮在所述程序存贮器中的预先安排的卡保密程序, 该程序用于为进行与交易相关的数据读出和写入操作而对保密保护存贮单元的持卡人存取保密性和终端存取保密性进行管理,

所述操作上兼容的终端包括与所述预先安排的卡保密程序兼容的预先安排的交易保密程序;

所述方法包括以下步骤:

a. 在所述 IC 卡中建立一个到所述数据通讯接口的卡数据链路;

b. 经由所述卡数据链路向所述 IC 卡传送一条持卡人数据保密信息, 以使得所述卡保密程序产生保密的持卡人识别数据;

c. 建立到所述运行兼容的终端的一个数据链路;

d. 经由所述卡数据链路和所述终端数据链路在所述 IC 卡和所述外部终端之间传输保密的交易信息, 包括从所述持卡人来的标记变化向量数据, 以使得所述 IC 卡和所述外部终端执行相互认证功能以及进行一个保密的标记值改变交易;

e. 经由所述卡数据链路读出存贮在所述 IC 卡中的一个修改后的标记值;

f. 将所述修改后的标记值传送到所述持卡人。

2. 根据权利要求1所述的方法,其特征在於进一步包括以下步骤:

a. 1. 在所述步骤a之后立即读出一个存贮在所述IC卡中的当前标记值;

a. 2. 将所述当前标记值传送到所述持卡人;

其中所述步骤b. 只有在所述持卡人启动一个标记值改变请求后才执行。

3. 根据权利要求1所述的方法,其特征在於存贮在所述IC卡中的所述标记值是一电子现金标记,所述方法适用于在所述私人场所进行由音频电话启动的与具有相关的操作上兼容终端的送货服务商业部门进行的持卡人购物交易,并且其中

所述步骤a是在所述持卡人向与所述送货服务商业部门相关的操作人员传送了声音购物订单后执行,以及

所述步骤c由所述持卡人和所述操作人员分别从音频电话链路切换到终端数据链路来执行,以完成所述方法步骤的结余。

4. 根据权利要求1所述的方法,其特征在於所述IC卡包括若干标记值数据项的保密保护存贮单元,每个数据项相关于某项服务,以及包括存贮在所述程序存贮器中一个预先安排的标记值初始化程序,该程序与所述远程位置处所述操作上兼容终端中包括的一个相应的预先安排的标记值初始化程序相兼容;以及其中所述步骤d包括:

d1. 从所述持卡人向所述IC卡和所述外部终端传送一个标记启动请求,并同时传送一个包括由所述持卡人请求的初始标记

值数额的一个标记变化向量;

d. 2. 经由所述卡数据链路和所述终端数据链路, 为所述 IC 卡和所述外部终端中的所述相应的标记值初始化程序, 在所述 IC 卡和所述外部终端之间传输保密的交易数据信息。

5. 根据权利要求 1 所述的方法, 其特征在于也适用于在所述私人场所进行若干自动银行业务交易, 其中

所述 IC 卡进一步包括若干银行帐号数据项的保密保护存贮单元, 包括储蓄、核算、信贷以及贷款帐目数据项的其中一项或多项;

所述操作上兼容终端有到与所述持卡人有关的银行的主机的保密数据和程序的连接, 并且其中所述步骤 d 包括经由所述卡数据链路和所述终端数据链路在所述 IC 卡和所述外部终端之间传送保密的交易信息, 包括与由所述持卡人选定的一系列所述标记值改变和所述自动银行交易中的一项或多项相关的交易信息。

6. 通过与一远程位置的运行兼容的终端进行联机交易对话, 在私人场所执行一项包括改变存贮在持卡人的 IC 卡中的标记值的交易的一个终端,

所述 IC 卡具有一个微控制器和相关的微控制器程序存贮器, 标记值数据和卡保密数据的保密保护存贮单元, 一个数据通讯接口, 以及存贮在所述程序存贮器中的预先安排的卡保密程序, 该程序用于为与交易相关的读出和写入操作而对保密保护存贮单元的持卡人存取保密性和终端存取保密性进行管理,

所述操作上兼容的终端包括一个数据通讯接口和与所述预先安排的卡保密程序兼容的预先安排的交易保密程序;

所述终端包括:

在所述 IC 卡中建立一个与所述数据通讯接口的卡数据链路的装置;

用于接收持卡人输入的一个保密数据项,并且经由所述卡数据链路向所述 IC 卡传送所述保密数据项的一个代表,以使得所述卡保密程序准备并且向持卡人送回卡认证数据项的装置;

为了使所述持卡人启动标记值变化交易的装置,其中要包括用于接收持卡人输入的一个标记变化向量的装置;

响应所述持卡人启动的标记变化交易,用于建立一个与远程位置的外部终端的终端数据链路的装置;

经由所述卡数据链路和所述终端数据链路在所述 IC 卡和所述外部终端之间传输一个预先安排的信息的装置,该信息包括:

使得所述 IC 卡和所述外部终端执行相应的终端认证和 IC 卡认证程序的保密认证信息;以及

保密交易信息,包括所述标记变化向量和使得所述外部终端证实持卡人身份并使所述 IC 卡和所述外部终端执行秘密的标记值变化交易的持卡人认证数据;

经由所述卡数据链路读出所述 IC 卡中经修改后的标记值并且将所述修改后的标记值传送到所述持卡人的装置。

7. 根据权利要求 6 所述的终端,其特征在于进一步包括:

在所述卡数据链路建立之后立即读出存贮在所述 IC 卡中的一个当前标记值的装置,以及将所述当前标记值传送到所述持卡人的装置。

8. 根据权利要求 6 所述的终端,其特征在于:

存贮在所述 IC 卡中的所述标记值是一电子现金标记; 并且所述终端适用于在所述私人场所进行经由一个音频电话启动的与具有相关的操作上兼容终端的送货服务商业部门进行的持卡人购物交易, 并且所述装置响应持卡人启动的标记变化交易包括用于在音频电话链路和终端数据链路之间切换的装置。

9. 根据权利要求 6 所述的终端, 其特征在于:

所述 IC 卡包括若干标记值数据项的保密保护存贮单元, 每个数据项相关于某项服务, 以及包括存贮在所述程序存贮器中的一个预先安排的标记值初始化程序, 所述程序与所述远程位置的所述操作上兼容的终端中包括的相应的预先安排的标记值初始化程序兼容;

所述终端进一步包括:

用于接收由持卡人输入的一个标记值初始请求以及一个相关的标记值变化向量的装置; 并且其中

用于传送一系列保密信息的所述装置包括传送保密的交易信息, 该信息中包含由所述 IC 卡和所述远程终端中的所述标记值初始化程序请求的所述标记值初始化请求及所述相关的标记变化向量。

对存贮在 IC 卡中的标记值 作再估价的系统和方法

本发明的背景

本发明一般相关于对存贮在 IC (识别码) 卡——也称作智能卡——中的标记信息 (诸如“电子货币”或“服务使用信贷”如电话使用信贷) 联机进行再估价的系统和方法, 详细地说, 相对于对一私人场所中进行这种再估价的系统和方法。

IC 卡的一种公认用途是存贮标记信息, 使持卡人在作非现金交易时使用。用于该目的的 IC 卡及其相关的交易终端采用了日益复杂的保密系统, 来防止未经授权制造卡、发行卡, 或欺骗性地使用卡。例如, 参看 Nakano 的美国专利 4, 810, 862 和 4, 839, 504, 这两篇专利介绍了在 IC 卡的制造与发行过程中引进、其后在认证卡及持卡人时采用的保密特征。

一些商业应用发行的一个 IC 卡带有一个初始的标记值以及卡逻辑或编程设计, 它只允许递减存贮的标记值, 直到完全用光, 此后将该卡弃置, 必须再买一张新卡。

其它商业应用发行的一个 IC 卡带有一个初始的标记值以及允许再估价, 即不仅能减少标记值, 也能使其增加的卡逻辑或编程设计。这些应用已众所皆知, 人们通常称其为“电子钱包”。

在某些电子钱包应用中, IC 卡只能在保密的再估价站作再估价, 例如完善的自动化出纳机 (见上述参考专利中 Nakano 的

US 4839504), 或与一台技术先进的主机联机运行的专用资金传输终端(见 Mansvelt 的美国专利 5, 175, 416)。这些保密的再估价站能够充分地利用卡和终端的保密特征, 并且通常保持在保密环境下, 以防止欺骗性使用以及阻止未经授权使用技术先进的探测保密特征, 这些保护特征在其后可能被用于关闭作为欺骗性卡发行或再估价系统一部分的再估价站。

IC 卡作为电子钱包使用的一个局限性, 是持卡人在用它完成交易之前不能容易地确定卡中剩余的货币标记值。如果存贮的货币标记值不足以支付购买值, 持卡人就必须取消这桩交易, 或者用其它方式支付。另一个局限性是持卡人通常必须到有专门的终端地点往卡里增加货币标记值, 使得使用电子钱包的方便程度和在 ATM (自动出纳机) 提取实际货币 (即政府发行的证券) 一样。

允许一电子钱包 IC 卡在一私人处, 如家庭或办公室中进行再估价的需求在 Ugon 的美国专利 4, 656, 342 中已被认可。该专利也考虑到通常需要将若干标记结合在一张电子钱包 IC 卡中, 并且每个标记与由一授权单位所提供的一项特定服务相关。除了通常为用于在经授权的电子钱包交易终端处购买货物和享受服务而存入的一个现金标记值外, 电子钱包也可以有如电话使用标记值, 它可以在装有已授权的 IC 卡接口设备的公用电话上使用。

在 Ugon 的美国专利 4, 656, 342 中描述的电子钱包再估价过程包括将基于声音的通话与专门的接线员结合起来, 以请求该专门的接线员对持卡人的电子钱包 IC 卡中的现金标记值或其它已授权的标记值作再估价。这样, 接线员和持卡人在持卡人所在处

的一个 IC 卡接口单元和接线员所在之处的一个授权终端之间建立了一个电话数据链路,从而接线员允许使用该授权终端和持卡人的卡接口单元来执行专门的卡和服务认证功能,如果成功地执行该功能后,那么就会导致 IC 卡自身将一个新的标记值写入到相关的标记值存贮单元。

本发明的目标

本发明的一个主要目的是提供一个改进的系统和方法,用于由持卡人在私人场所对 IC 卡上存贮的一个或多个标记值作再估价。本发明的另一个目的是提供一个改进的私人交易终端,用于执行与 IC 卡相关的交易操作。

本发明的特性和优点

本发明的一个方面描述一种方法的特征,该方法通过与远程操作上兼容的终端进行联机交易对话,实现在私人场所将向持卡人发行的 IC 卡中存储的标记值作出改变。该方法采用的 IC 卡具有一个微控制器及相关的微控制器程序存贮器、用于标记值数据和卡保密数据的保密保护存贮单元、一个数据通讯接口、以及存贮在所述程序存贮器中的预先安排的卡保密程序,这些都是为了在与交易有关的数据读出和写入操作时,对持卡人和终端向保密保护存储单元存取进行保密管理。

在远程处的操作上兼容的终端包括一个数据通讯接口和与所述预先安排的卡保密程序兼容的预先安排的交易保密程序。

应该理解, IC 卡既可以只存储一个标记值,即一个现金标记,也可以有许多标记值。还应该理解,“IC 卡”和“智能卡”两个术语可以交替地用来描述本发明。

本发明的方法包括: 首先, 在所述 IC 卡中建立一个与所述数据通讯接口的卡数据链路, 接着, 经所述卡数据链路将持卡人数据保密信息传送到所述 IC 卡, 使得所述卡保密程序产生保密的持卡人识别数据。该方法也包括在远程位置建立一个与一外部终端的终端数据链路, 然后经由所述卡数据链路和所述终端数据链路, 在所述 IC 卡和所述外部终端之间传送保密交易信息, 包括来自所述持卡人的标记变化向量数据, 使得所述 IC 卡和所述外部终端执行相互认证功能并进行保密标记值变化交易。

当 IC 卡和远程终端之间的交易完成之后, 该方法继续进行, 经由所述卡数据链路读出一个存贮在所述 IC 卡中的修改了的标记值, 然后将所述修改了的标记值传送到所述持卡人。通过使所有的安全认证和交易信息数据项目都出自 IC 卡自身, 并且经由一个远程数据链路简单地传送这些信息, 本发明的方法能够以简便的方式对 IC 卡的标记作远程再估价, 并且便利在交易的持卡人端使用简单便宜的硬件。本发明的另一方面描述了一个用于在私人场所进行一桩交易的终端特性, 该交易包括通过与一远程位置的一个操作上兼容终端进行联机交易通话向一持卡人发行的存储在 IC 卡中标记值作出改变。该 IC 卡和操作上兼容终端具有上面所描述的特性。

持卡人使用的私人终端包括在所述 IC 卡中建立与所述数据通讯接口的一个卡数据链路的装置, 以及用于接受一个保密数据项的持卡人入口, 并且将所述保密数据项经由所述卡数据链路传送到所述 IC 卡, 以使得所述卡保密程序准备并返回持卡人和卡认证数据项的装置。

私人终端另外还包括用于使所述持卡人启动一桩标记值变化交易的装置,其中包括用于接受标记变化向量的持卡人项目的装置,以及响应所述持卡人启动一个标记变化交易的装置,此装置用于经由一个公共交换电话网络建立与一远程位置的一个外部终端的终端数据链路。

私人终端的另一部件是经由所述卡数据链路和所述终端数据链路在所述IC卡和所述外部终端之间进行一系列保密信息传送的装置。这些信息包括使所述IC卡和所述外部终端进行各自的终端认证和IC卡认证程序的保密认证信息,以及包含所述标记变化向量以使得所述IC卡和所述外部终端能执行一个保密的标记值变化交易的保密交易信息。

私人终端还包括经由所述卡数据链路读出一个存贮在所述IC卡中的修改了的标记值、并将所述修改后的标记值传送给所述持卡人的装置。该传送装置可以是一台字母数字显示器,或一台打印机,或一台计算机产生的声音读出器。

本发明的私人终端具有简单、便宜的优点,因为IC卡和远程终端构成所有的保密信息,并且用主要起信息传送机构作用的私人终端来处理被编程的交易活动。由于私人终端自身不能与IC卡相互作用来进行任何交易活动,这就减小了欺骗的危险。该私人终端不必保持在保密环境中,因而这种终端可以分布在持卡人家中、办公室中和其它私人场所使用。

本发明的私人终端也并非仅供特定的持卡人使用,而是可以由持有可兼容IC卡的任何持卡人使用。因此,尽管私人终端可以做成手持式的,但没有必要这么做。在每个办公场所的一台唯一

的终端可供许多持卡人使用,来读出他们的卡上的标记值,以及采用该终端的设施,根据需要来重新估价标记值。

在IC卡上存贮了远程终端电话号码和其它银行数据后,私人终端能基本上起到无声通讯终端的作用,用于其它银行交易以及在IC卡上的标记再估价。一旦在一保密的基础上远程终端和IC卡交换了帐号和其它数据后,远程终端和私人终端能与远程终端提供的银行功能信息和由持卡人所作的功能选择交互作用。当然,在私人终端为个人ATM型交易提供的智能等级是任选的。例如,私人终端可以包括有关结帐审核、小型财务报表核算、存款和支票付款核算等等基本的功能键。

本发明的其它目的、特征和优点,根据下面本发明实施例所作的详细描述会得到清楚的了解。

附图的概要描述

图1的基本系统图示出了关于本发明的有用的现有技术的卡发行系统的一些单元;

图2A和2B的基本系统图示出了关于本发明有用的现有技术的交易系统点的一些单元;

图3是本发明的私人再估价和交易系统的一个基本系统图,该系统在实施本发明的方法中是有用的;

图4的方框图示出了根据本发明并实施本发明方法的一个系统的单元和模块;

图5示出了根据本发明一个智能卡数据连接结构有用的一部分;

图6A-6C的流程图示出了根据本发明在私人终端执行的

方法步骤;

图 7A 和 7B 的流程图示出了根据本发明在智能卡中执行的方法步骤;

图 8 的流程图示出了根据本发明在一主机中执行的方法步骤。

发明实施例的详细描述

图 1 示出了有关本发明特别有用的卡发行系统的全部单元。例如, 美国专利 5, 175, 416、4, 810, 862 和 4, 968, 873 详细描述了 IC 卡的发行, 这些细节在描述本发明背景时作为参考被编进去。

一般说来, IC 卡发行是由终端 10 进行的, 它包括或连接到智能卡读出/写入装置 11, 智能卡 12 可以被插入到装置 11 中。在这种情况下, 智能卡 12 是这样的: 若干标记值可以被记录在其中的若干单独的标记存贮单元, 每个标记值相关于一项特定的服务或交易机构, 如一电子现金标记与银行 A 14 相关, 一个商店常客标记与一商店常客服务 15 相关, 一个电话使用标记与一电话公司 16 相关。智能卡 12 也可以有保密帐号存贮单元, 使它能够同时具有信用卡和借方卡或其中之一的功能。

终端 10 连接到主机系统 13, 主机 13 中有与上面描述的每个服务机构的交易数据链路。持卡人可选择发行给他的智能卡装入一个或多个可用的标记。装入一个现金标记和装入一个电话使用标记, 每一种都包含与银行 A 的交易, 以便将装在卡上的标记值记入持卡人的借方帐中。就电话公司的情况而言, 电话使用标记的值在它被记入持卡人借方帐中的同一时刻被记入电话公司的贷方帐中。装入到卡中的现金标记值可由银行在关闭的卡系统中

将其保存在特定的暂存帐号中或在开放卡系统中被转送到一个结帐或清算机构。卡发行的这一记帐方面不是本发明的实质，因此在此不作详细讨论。

本发明重要之处是装有这些标记值的智能卡被制造成带有多个标记存贮单元的一种型号，这些存贮单元具有适当的保密级别，智能卡自身也具有保密特征，例如信息的加密/解密、卡对终端的认证、以及根据本发明进行标记值再估价的编程设计。多标记值或多帐号智能卡在例如美国专利 4, 656, 342 和 4, 736, 094 中都有公开，为了显示一个具有多标记值存贮能力的 IC 卡的示例结构和功能，将上述两篇专利文献被编入进去作为参考文献。

可被用来实施本发明的一种特殊形式的智能卡是在 PCOS 技术说明书(第 1.0 版，由法国 GemPlus Card International of Gemenos Cedex 出版)中描述的 PCOS 智能卡。在需要表示 IC 卡的示例结构和功能时，也将这篇文献编入进去作为参考文献。

卡的使用

作为背景资料，图 2A 示出了典型的现有技术卡在交易场所的一个点使用的情况。交易终端站 20 能够采用磁条卡进行借贷型联机交易，也能采用电子钱包型的智能卡 12 脱机进行借方型交易。

对联机交易而言，终端 20 有一个可用来读一磁条卡 25 的磁条卡阅读器 21。对这种联机交易来说，终端 20 有一个经由公共电话网络(或租用线路)到主机 27 的数据通讯链路，用作信贷认证或借方交易处理。图 2A 的系统也包括一个智能卡读出/写入模块 22，该模块也包括一个用作 PIN 入口模块来输入用于认证持卡人

的个人识别号码的键板。如果智能卡12中装入了现金值标记,那么它可以用来在脱机交易中支付购买的货物或得到的服务。在这种脱机交易的典型步骤中,首先是根据存贮在卡12中的相应数据,通过请求一个PIN入口及其确认,使终端20和插接板22对持卡人加以认证,从而避免由未经授权的人欺诈性地使用卡12。

在某些电子钱包应用中,为了加快交易处理速度,可以取消该PIN确认,不过这不是强制性的。在这种情况下,电子钱包被当作现金一样处理,持卡人被假定为电子钱包的真实所有人。用于没有PIN入口的电子钱包借方操作的销售终端站的一个例子在Roberts等人的美国专利申请08/143,573中作了公开,该申请于1993年10月26日提交,发明名称为“电子现金交易方法及其设备”,它与本申请被转让给同一公司,目前处于待审查阶段。

另一种选择是仅仅当交易额超出预选的底线时才请求PIN项以便花费电子钱包中的金额。

接着,终端20和卡12通过一个相互认证过程来彼此证实,该过程检查卡和终端的真实性以及相互兼容性。这种相互证实能防止采用欺诈性发行的卡来进行交易,也能防止使用未经许可的终端从卡12中提取或向卡12中增加款项。一旦完成保密认证,终端20和卡12就来回传送交易信息,使得从卡12中提取的币值进入终端20的交易项目存贮器,并且将一个新的现金值重写到卡12中。这些步骤是大家都知道的,在此不必作详细讨论。

此后,终端20可能呼叫主机27或主机13,或同时呼叫二者,采用各种付款卡媒体对一天的交易进行结帐。采用智能卡12作为现金标记媒体和等价的政府发行的纸币的临时性证券,其优点

是它具有脱机交易的特性,并且能避免实际的现金交易以及由于找钱、核算备用金等造成的时间浪费。

如果智能卡 12 有一相关于某个商家的常客示记,即与该商家进行交易,那么该交易也可以包括证实商店常客标记的步骤,并且,如果适当的话,根据交易额改变卡 12 上的常客标记值。根据常客程序的特性,卡 12 中的标记值可以用于给当前购物折扣或类似行为,例如根据资金积累到一定程度恢复奖励。

图 2B 示出,如果智能卡中装有电话使用标记值的话,智能卡 12 也可以用在公共电话亭 29。在这类应用中可以包括同样的交易步骤。另一方面,可以采用不太保密的交易步骤,例如假定持卡人是一个获授权的所有人,以便使得智能卡 12 与打电话的单一模式智能卡兼容,后者只为保密目的核实卡的真实性。

在私人场所再估价

图 3 示出了本发明的一般原理。该发明提供了采用终端系统,在很少保密或不保密的情况下,在“私人”场所对智能卡现金标记值作重新估价的方法和设备,这与在公共场所进行的重新估价完全不同,在公共场所采用了物理与电子两方面的高程度的系统保密性。

参看图 1,很显然,包含在卡发行中的硬件,无论从硬件存取还是运行的角度来看,其维护都必须在保密设施中进行,以避免欺诈或未经授权的行为。如图 3 所示,通过在终端中包括对卡作再估算和发行所需要的任何应用软件,可以在卡发行与再估算站 10A 完成对智能卡的再估算。包括同样的设施以及采取同样的保密条件,可以实现卡和终端之间进行两者之间的相互认证。也可

以要求持卡人在一台单独的输入设备上秘密输入他的 PIN, 或者经过训练的受委托操作员可以输入 PIN, 并且也进行银行交易协议中可能包括的其它持卡人认证步骤。

除了持卡人正在进行交易步骤外, 也可以在为智能卡再估算功能而设置的任何公共 ATM 单元 36 进行同样的保密步骤。

图 3 也示出了采用“私人”终端 30 对卡作再估算的情况。私人终端 30 可以设在持卡人家中、办公室或其它场所, 如宾馆饭店的前台或门房。总的原理是采用具有智能卡数据接口的一个简单终端 30, 通过调制解调器或其它数据通讯媒体, 与智能卡 12 和远程终端数据链路进行通讯, 该远程终端可以是主机 13 自身, 或者是一个网络存取控制器 40, 并且该远程终端被编程, 用于在 IC 卡 12 和远程终端之间传送保密信息。这里所用的名词“保密信息”指的是采用加密方法或其它手段, 使得信息在 IC 卡和/或远程终端保密, 而不是在终端 30 保密。从本质上说, 终端 30 在 IC 卡 12 和远程终端之间提供了一个链路, 它等同于在 IC 卡 12 和保密卡再估算站中的终端之间存在的硬接线数据通路。终端 30 在两个单元之间传送数据和命令信息, 并且它的操作系统在智能上可能只限于管理该简单功能。当然, 也可以包括更复杂的功能, 使得终端能处理其它 ATM 或远程用户服务功能, 当已经在 IC 卡 12 和远程终端之间对所有的保密信息的发射和接收都处理之后, 这些功能不需要起始产生和接受保密信息。

图 3 也示出可以给简单的私人再估价终端 30 提供硬件和智能, 以参与与邮购机构 35 的电话邮购订单交易。由于给出信用卡号码会导致由邮购公司的职员或截取信息的某人欺诈性地使用,

因此,作为一种替代形式,可以给终端 30 提供一种能力,使它能暂时从声音切换到数据,以执行 IC 卡借方功能。然而,保密功能仍然在 IC 卡和远程终端——在这种情况下可能是网络存取控制器(NAC)40——之间执行,因而私人终端 30 或邮购机构的终端都不必有复杂的保密特征。在这种情况下,网络存取控制器被编程以执行简单的借方交易,它将 IC 卡 12 的现金标记中的现金交易借方额需要的信息和参数传送到私人终端 30,并将贷方交易额的其它信息传送到邮购机构。此后,NAC 40 通过电子声产生的信息或一数据显示信息告之各方,电子交易完成。根据编程设计,NAC 40 然后可以终止电话连接或回复声音通讯各方停止讲话。

很显然,这种 IC 卡再估价功能和订购交易功能也可以包括在家庭终端设备中,该设备还提供了在家庭购物或家庭交易网络环境下的额外的智能功能。例如,这种再估价功能也可以在被编程的一个智能屏幕中实现,以执行与个人终端 30 相同的功能。

IC 卡最好是存贮终端 30 需要的所有信息,以便在不与持卡人交互作用的情况下对远程终端数据链路进行初始化。如果需要的话,这可能要包括主电话机号码数据和银行帐号数据。另一方面,IC 卡识别号也可以直接连接到一个单一帐号或帐号组。

另外,由终端 30 呼叫的电话号码最好是为私人终端 IC 卡再估价功能专用,以避免要求个人终端 30 发出一个特别的登记信息来指示请求什么类型的交易。然而,使用有由个人终端 30 提供的登记的通用主电话机号码也在本发明的总原理之内。显然,一旦保密帐号和持卡人的识别(PIN)信息已经在 IC 卡 12 和远程终端(主机 13 或 NAC40)之间传输后,可以在终端 30 和主计算机之

间进行附加的 ATM 或顾客服务咨询交易。这种功能的智能可以全部装在主机上, 在私人终端 30 仅仅安装显示和键盘 I/O 命令解释器。另一方面, 可以由主机和私人终端 30 分享智能。例如, 根据专用的功能键或通过卷动屏幕所进行的菜单选择或其它手段, 可以对私人终端 30 编程, 使得用户将交易初始化信息或数据查询传送到主机。

现在可以清楚地得知, 本发明的一个私人终端 30 可以广泛地分布在人们家中、办公室和其它场所, 而不会冒泄漏 IC 卡或远程终端的保密的风险。此外, 每个持卡人可以有使用任何私人终端 30 来再估价 IC 卡中的现金标记值的优点。

系统例子

图 4 以方框示意图形式示出了在构成本发明的私人终端再估价系统时通常采用, 并且能执行本发明方法的模块。

私人终端 30 有一微处理器系统 60 及相关的程序存储器 61、数据存储器 62、以及输入/输出设备, 如键盘 63、显示器 64、调制解调器 66 以及智能卡数据链路 65。如果系统提供了用于银行服务和/或邮购订货业务的组合声音—数据交易的话, 那么也可以包括一个声音—数据开关 67。智能卡数据链路 65 可向智能卡 12 提供数据通讯业务, 也可以用于向智能卡 12 提供 DC 操作电能。智能卡 12 有一个装载板和/或辅助程序的内部微控制器 70, 和数据存储器 71 和 72。数据通讯由数据 I/O 74 和加密/解密模块 73 一起处理, 该加密/解密模块 73 可以是硬件, 也可以是软件。

在主机一边的一个专有卡系统中, 主机 13 有一个控制生成保密认证和交易信息与功能的智能卡保密模块和一个与智能卡

12 中的类似功能兼容的加密/解密模块 76。

在一开放型卡系统中, NAC 40 有一个智能卡保持密模块 81 和加密/解密模块 82。声音数据交易控制 83 提供关于银行 B 的 NAC 的声音与数据接口的操作, 银行 B 采用声音进行顾客业务, 邮购机构 35 以声音起源购物结算的形式从智能卡 12 接受电子现金。

图 5 示出了现有技术的智能卡数据连接设备 65 部份, 它具有 IC 卡读出/写入接口单元形式, 其中, 卡插入传感器 90 感应什么时候智能卡 12 完全插入到读出器的卡接收腔, 并完成与卡的接触, 以便将电能施加到卡上。

读出结余 - 增加现金程序和有关的智能卡及主程序步骤

图 6A - 6C 示出了在私人终端 30 运行的命名为“读出结余 - 增加现金 (READ BALANCE - ADD CASH)”的程序的步骤。该程序的主要步骤的目的是将现金支出加到智能卡 12 中的现金标记上, 为解释起见, 假定 IC 卡按“PCOS 技术说明书”(由法国 GemPlus Card International, Gemenos Cedex 出版) 中规定的 PCOS 智能卡的电子钱包说明书来操作。该 PCOS 说明书描述了现有技术中采用终端对用户输入的 PIN 进行加密以及也对从主机接收的信用密码电文加密的方法。根据本发明, 终端没有加密保密程序, 所有加密操作都在智能卡 12 和主机中进行。如图 6B 及下面所述, 终端可以进行 XOR 功能操作, 以设置智能卡 12 的 PIN 加密操作。另一方面, 也可以将代码加入到智能卡 12 上, 以进行全部的 PIN 加密操作。

该程序模块的第一步是在读出器 65 中检验卡的存在, 该步

骤循环进行,直到感应到卡为止。当检验步骤的结果为肯定时,程序向智能卡 12 供电,并且向 IC 卡传送一个复位命令。此卡向私人终端 30 作一答复,由该答复可识别卡的类型。下一步即检查接收的答复是否指示 IC 卡是一个 PCOS 卡。如果回答为否定,那么表明有错,并在私人终端 30 的显示器上显示适当的错误信息。如果回答是肯定,那么向智能卡传送一个结余(现金)(BALANCE (CASH)) 命令。智能卡作出一个简单的查找存贮在卡的现金标记存贮单元中的值的响应,并且经由两个设备之间的通讯链路将该值返回到私人终端 30。

应该理解,传送到智能卡 12 的每个命令之后都跟随一个 Get Response (得到响应) 命令。另外,根据实践,对于一个好的软件来说,当每个 GetResponse 命令发出之后,要包括一个响应超时功能(没有示出)和一个响应有效功能(没有示出)。响应超时功能首先包括启动一个计时器,然后依次检查看看是否已接收到一个响应,或计时器是否已满,如果在接收到响应之前计时器已满,那么声明出错。

如果在超时之前发回一个响应,那么在一单独的检验步骤中检验该响应的有效性。如果该响应无效,那么声明一个适当的错误。在描述此示例性程序的这些步骤中,假定私人终端 30 和智能卡 12 的硬件和软件运行正常,于是计时器和检查步骤的有效性将是满足的。

接下来,在显示器 64 上显示从智能卡 12 接收到的现金结余 (Cash Balance),在此之后或与此同时显示一个“增加现金 (ADD CASH)?”菜单项。私人终端 30 最好有至少两个软件功能键,用

于对菜单显示的肯定和否定答复。另一方面,也可以在键盘上包括肯定与否定共享或专用的功能键。

应该理解,在图 6A-6C 所示程序流程中的不同位置上可以包括检查智能卡 12 是否在超时发生之前拿走的步骤(没有示出)。如果没有进一步要求活动的话,这种做法将延迟后面程序的执行,以允许用户将卡取出。这种做法可能有用的一个地方是在显示了现金结余之后。如果用户正在检查现金结余。则可以在结余显示之后马上将卡取出。如果卡取出后,那么,执行将返回到程序开端,等待插入另一张卡。如本技术领域中所公认的那样,私人终端 30 将包括一个子程序,来感应取卡的过程,并且在与卡接触结构的实际通讯失去之前就对卡断电。换句话说,卡插入开关在终端与卡接触断开之前就感应到卡的移动,从而可以在实际接触切断之前就执行断电步骤。

注意,该现金结余读出和显示步骤是在没有任何保密步骤的情况下执行的,并且在卡入口上自动进行。这就使得持卡人只需简单地将卡插入私人终端 30,就可以检查他的智能卡上的现金结余。这一操作如同打开钱包看其中有多少钱一样快捷,它是根据本发明提供一个私人终端的主要优点。

下一步检查由用户所输入的回答。如果没有输入“是”,那么程序跳到图 6c 的点 D,确定用户是否要求了私人终端 30 的其它功能。假定用户希望将更多的现金记入到智能卡 12 中,判断步骤将作“是”的回答,私人终端 30 将传送一个命令到智能卡 12 上,请求它的 DDA#。

下一步是显示“输入 PIN”,接下来是接受用户所作的一个

PIN 代码号的键盘输入。接下来对输入的 PIN 作函数处理: $PIN_BLK = XOR(PIN, DDA\#)$ 。通过在私人终端30 执行这一功能, 在一 PCOS 智能卡中已经提供的加密码可以用于完成一 PIN 加密操作, 它将与主机中设置的进行现金信贷操作的 PIN 有效性代码兼容。

下一步是向智能卡 12 传送一个命令, 对 PIN_BLK 的值进行 PIN 加密。智能卡 12 的响应是执行图 7A 所示的程序步骤, 接收 PIN_BLK 参数, 然后执行一系列功能, 对 CTC (卡终端计数器) 增 1, 接着执行加密步骤, 采用称为 Kauth 的认证键, 将认证对话键 K_{sa} 设定为等于对 CTC 加密的结果, 接着又执行一个加密步骤, 采用通话键 K_{sa} 将经加密的 PIN 值 P 设定为等于对 PIN_BLK 参数加密的结果。随后, P 和 CTC 的值由智能卡 12 返回到私人终端 30。

接下来在私人终端 30 执行的步骤是接受并存贮 P 和 CTC 的值, 以便它们能包括在一个主机的信息包中。此后向用户显示一条提示信息: “AMT. TO ADD?” 接着接受一个输入值 Ca , 作为加到智能卡 12 的现金标记中的现金金额。应该理解, 选定要增加的金额可以多种方式进行。与某些 ATM 机一样, 私人终端 30 可以建议一种“即可兑现的现金”数额, 如 \$40.00。私人终端 30 可以追踪用户增加现金值的习惯, 并且建议用户选择的通常数额。这一步骤应理解为包括很宽范围的金额选择子过程。

当要增加的金额 Ca 被输入并接收后, 私人终端 30 向智能卡 12 发出一个命令, 得到主机的电话号码, 并与之通话, 来进行现金提取和卡信贷操作。这包括直接读取智能卡 12 中的一个存贮单

元或文件, 终端就知道了该智能卡 12 存贮的主机电话号码。应该理解的是, 卡中间能有其它标记, 并且其它主机的电话号码可能连接到这些标记, 例如, 商店购物奖金标记可能有与主机进行通话来花掉这些奖金的电话号码。

当私人终端 30 得到主机电话号码后, 它拨通该号码并与主机建立通讯连接。这可以通过采用公用电话线的调制解调器或蜂窝式调制解调器或任何其它数据通讯媒体来实现。当与主机的通讯联系建立起来之后, 私人终端 30 传送一个 WITHDRAWAL_CD_CRD 包, 告诉主机交易的类型以及包括的参数, 例如, 在这种情况下是 DDA#、P、CTC 和 Ca。

主机响应这一信息包所采取的典型步骤示于图 8。当主机收到 WITHDRAWAL_CD_CRD 信息包后, 它通过采用认证键 Kauth 对收到的 CTC 参数进行 DES 加密来驱动认证通话键 Ksa。PIN_BLK 是通过采用已被驱动的通话键对 P 参数进行 DES 解密来驱动的。这些是通话保密过程中的标准加密/解密行为, 在此不必作详细解释。如果 PIN_BLK 是有效的, 这意味着主机已证实了输入的 PIN 并且证明智能卡 12 在加密 PIN_BLK 时已采用了合适的认证键 Kauth。

后面完成这些功能, 主机运行一系列检测步骤, 看 PIN_BLK 是否有效, 以确定帐号中是否有足够的资金, 并且确定是否超出了交易限定参数, 例如每天的提取限额。如果这些检测步骤中有任一个返回的结果是“否”, 那么产生一个适当的错误信息包送回到私人终端 30 去处理。如果包括一个 PIN 输入错误, 那么可以更新 PIN_ERROR 计数值, 使得主机能确定用户是否采用无效的

PIN 输入尝试了许多次,以图进入帐户。

如果检测步骤都返送结果“是”,那么主机执行一系列功能。通过采用信用键 Kcre 对 CTC 进行 DES 加密来驱动主机对话密钥 Ksh。随后运算函数 XOR (Ca, DDA#),计算出信贷密码 CC。

接着,如附图中功能方框所示进行两个顺序解密步骤。通过采用主机对话密钥 Ksh 对 CC 进行解密,产生信贷密码电文的 CC' 版本,然后,通过采用认证对话密钥 Ksa 对 C' 进行解密,产生一个 CC'' 版本。接着,由主机将该 CC'' 值传送到私人终端 30,作为一个 VALID CC'' (有效 CC'') 确认包的一部分,当接到来自私人终端 30 的一个 DN_MSG 时,主机结束 (DONE)。应该理解,可以对私人终端 30 编程,使其在主机联机时能执行其它私人 ATM 功能。如果这样的话,主机将在私人终端 30 的命令下或响应不同的传输数据包执行其它私人银行交易步骤。这种附加的功能不是本发明的一部分。

再回到图 6c,私人终端 30 接受并检查主机信息。如果收到某类错误信息包,那么私人终端 30 确定交易已失败,显示一个适当的错误信息,并返回到初始程序步骤。根据失败的原因,用户可以再试一次。

假定该主机信息表明交易是成功的,私人终端 30 向智能卡 12 传送一个 CREDIT_CASH (支出现金) 命令,并带有命令参数 CC'' 和 Ca。智能卡通过执行图 7B 所示的 CREDIT_CASH 子程序,来处理这个命令。此命令参数被接收,并随后执行一系列功能,首先,通过采用认证对话密钥 Ksa 对 CC'' 进行 DES 加密,导出参数 CCa'。注意,这是如图 8 所示由主机执行的最后的加密操

作的逆操作。然后,通过采用信贷密钥 Kcre 对 CTC 作 DES 加密,产生主机对话密钥 Ksh。这在主机中模拟一个功能。接着,通过采用主机对话密钥 Ksh 对 CCa' 进行 DES 加密,导出参数 CCa。最后,通过对 CCa 和 DDA# 执行 XOR 操作,导出 Cac。

接下来检查智能卡 12,看 Cac 是否等于 Ca,因为如果智能卡 12 中的所有加密和解密操作都与主机中的相应操作相匹配的话,Cac 会等于 Ca。如果没发现这种匹配,那么向私人终端 30 返回一个错误信息。如果发现匹配,那么通过增加一个 Ca 值对现金标记中的现金结余予以更新。此后向私人终端 30 返回一个成功代码。

回到图 6c,假定 CREDIT_CASH (支出现金) 命令被发出并在卡中执行后,私人终端 30 从智能卡接受一个有效响应,那么再发出一条 BALANCE (CASH) (现金结余) 命令,此现金结余将与交易完成 (TRANSACTION COMPLETE) 信息一起又被显示出来,以使用户能核实新的结余中包括所请求的额外现金。

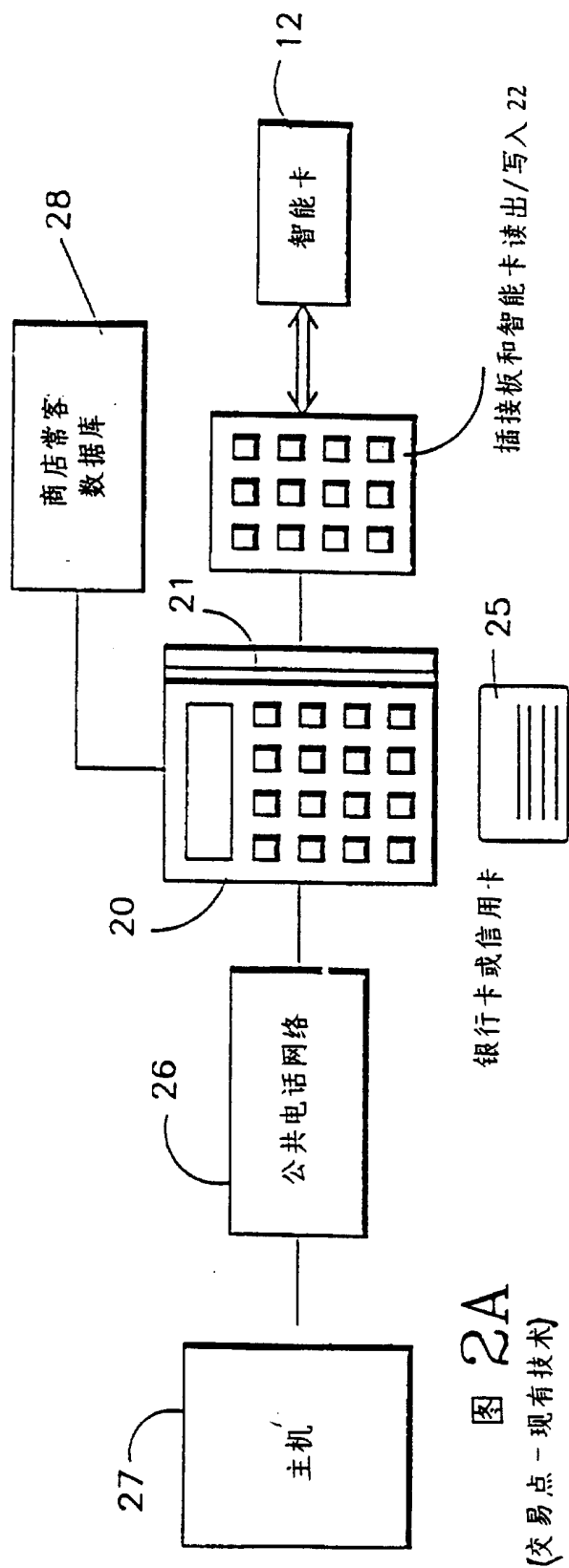
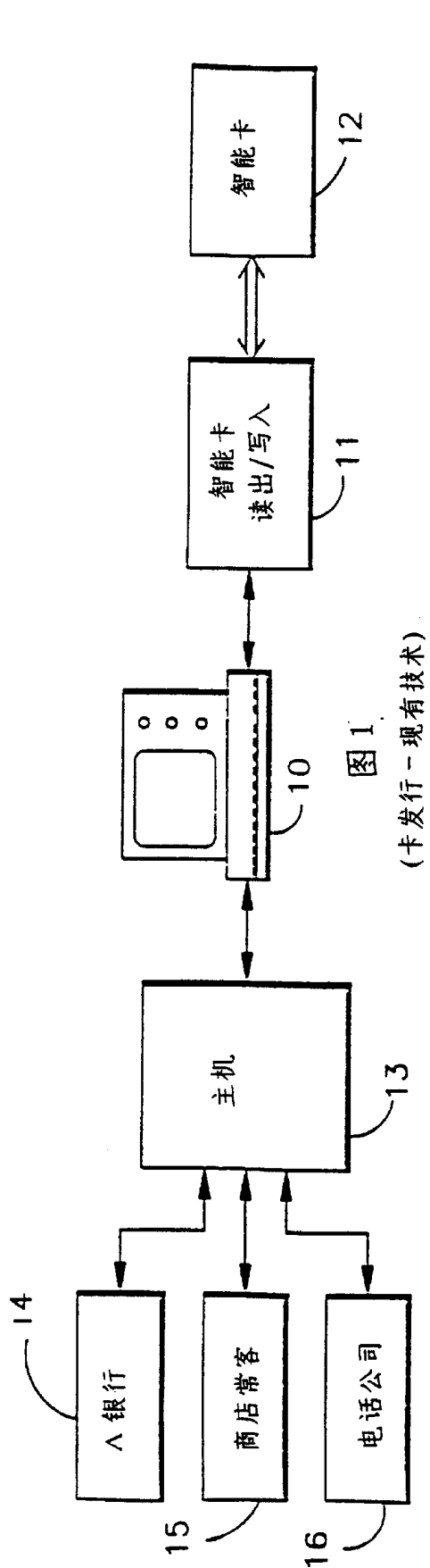
接着,程序检查是否有其它卡请求为用户所需要。如果没有,卡被断电,一条 DN_MSG 被传送到主机,并且程序返回到开始位置。如果其它卡请求没有被指示,那么程序检查用户是否指示了其它 ATM 请求。如果是,私人终端 30 执行这些个人 ATM 功能,直到用户完成所有交易为止。这种额外的个人 ATM 功能不是本发明的一部分,因此不在此进行讨论。它们可能包括由私人终端 30 在一银行处以模拟一个 ATM 机器的方式从一远处进行付帐、转帐等活动。

根据上面的描述,应该清楚,本发明的私人终端 30 可以是一个简单并且便宜的设备,因为它与智能卡 12 和主机进行简单的

数据输入和数据通讯工作。由于不需要采取保密措施来防止欺诈, 因此终端中没有保密功能, 从而终端的制造很便宜。

也应该理解, 对所示出并加以讨论的示例性程序可以作许多变化。例如, 在私人终端 30 中运行的程序可以包括一条给智能卡 12 的命令, 用于在执行其它步骤之前证实输入的 PIN。这会避免设置所有只与主机连接的步骤以发现在 PIN 输入中已有的错误。在这种改进中, 智能卡 12 可以包括一个检查 PIN 的模块, 以便在卡被锁住无法作进一步使用之前, 经用户几次机会试一试插入正确的 PIN。

本发明系统与方法的一般原理是通过描述各种实施例说明的。然而, 应该理解, 本领域的技术人员在不违反下面本发明的权利要求中所要求的范围的前提下可以作许多改进。



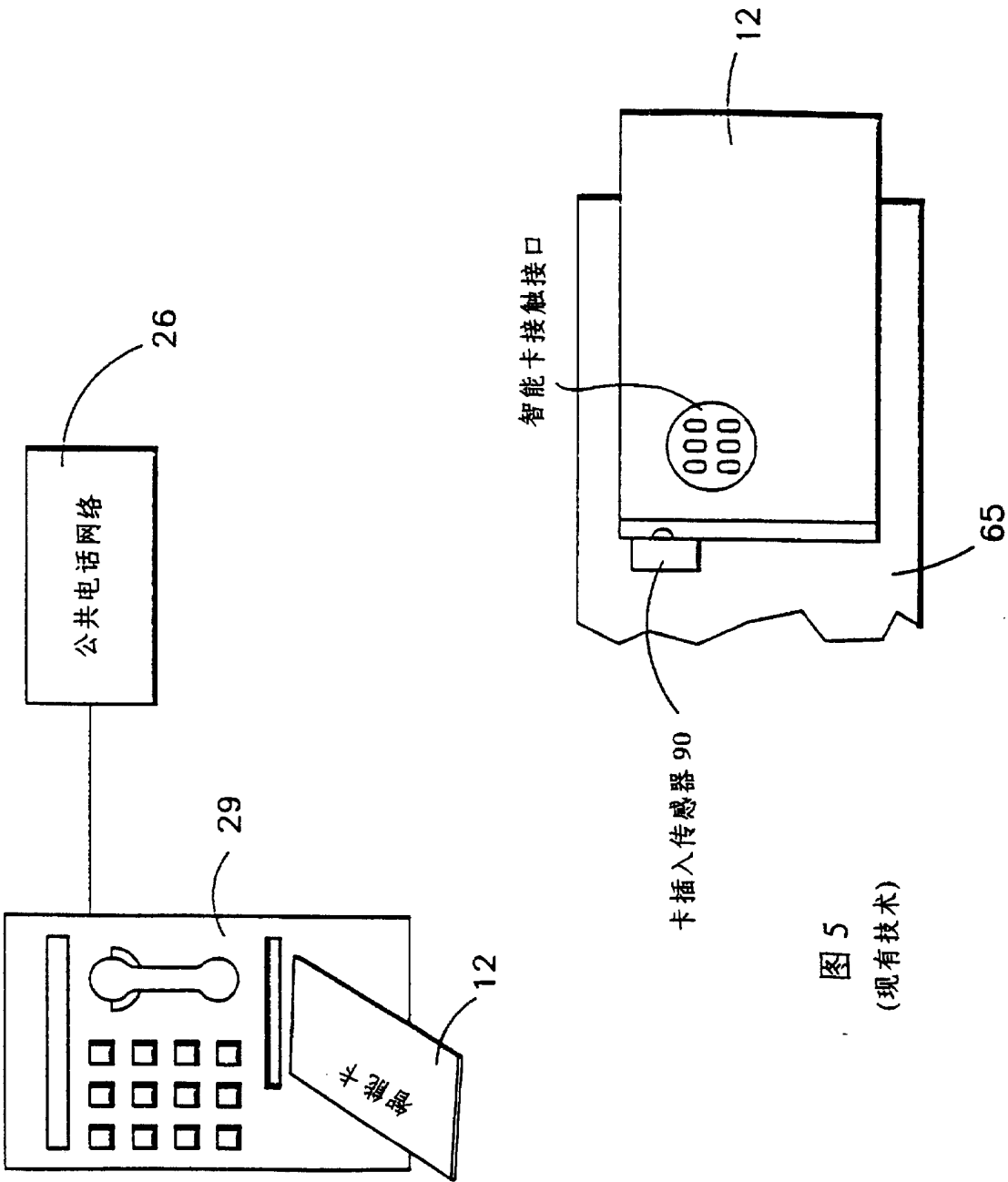
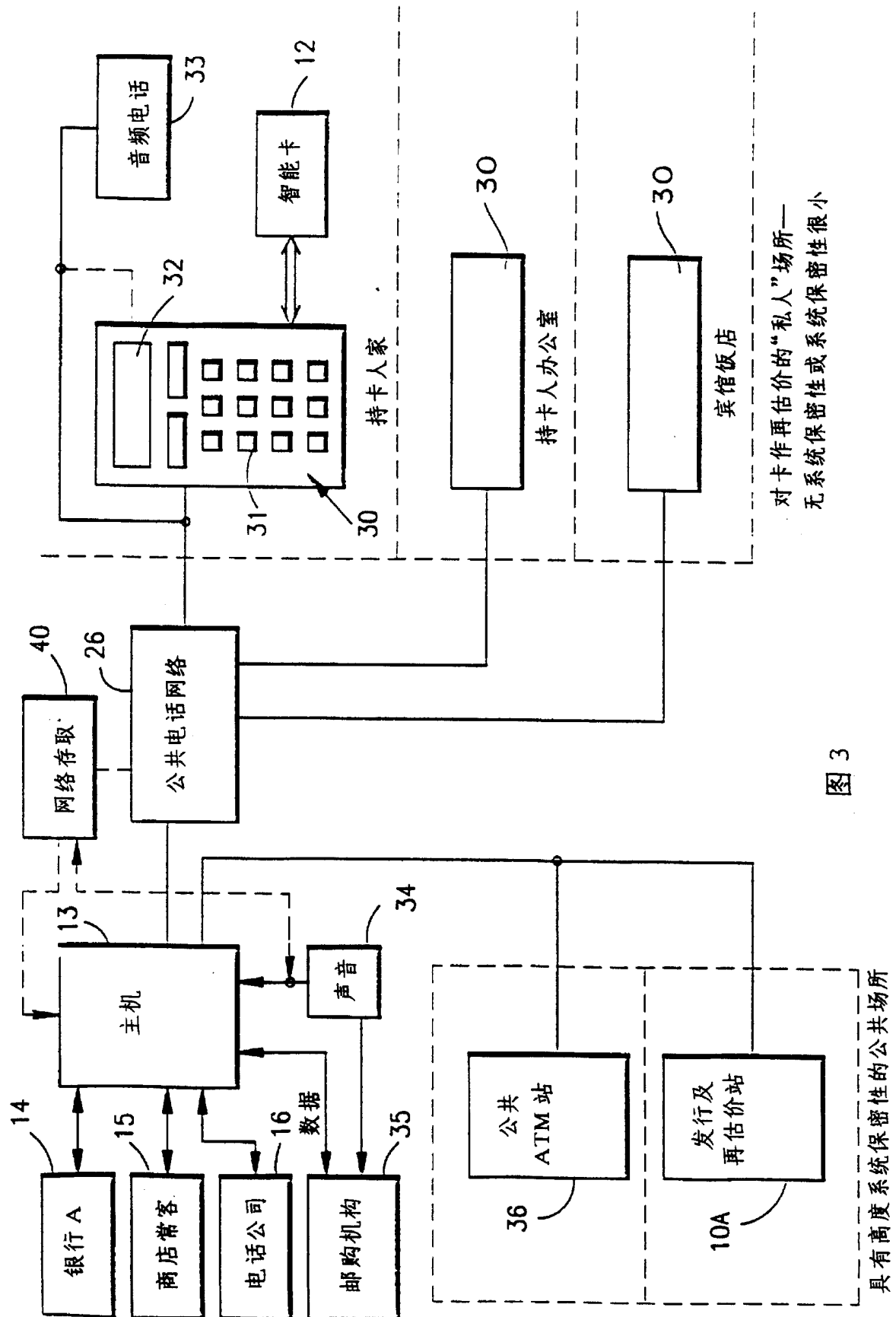
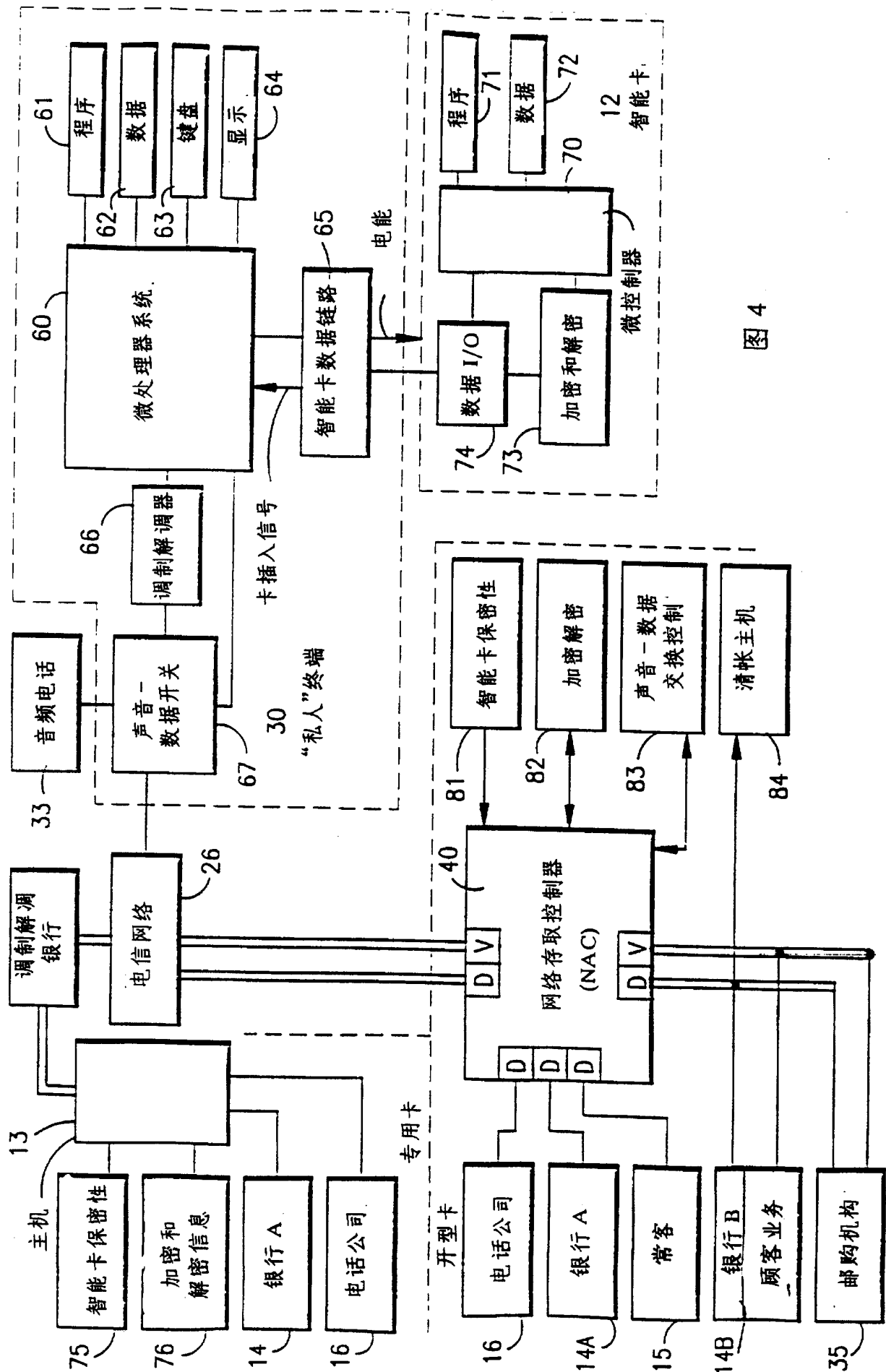


图 2B
(电话使用 - 现有技术)

图 5
(现有技术)



3
图



4

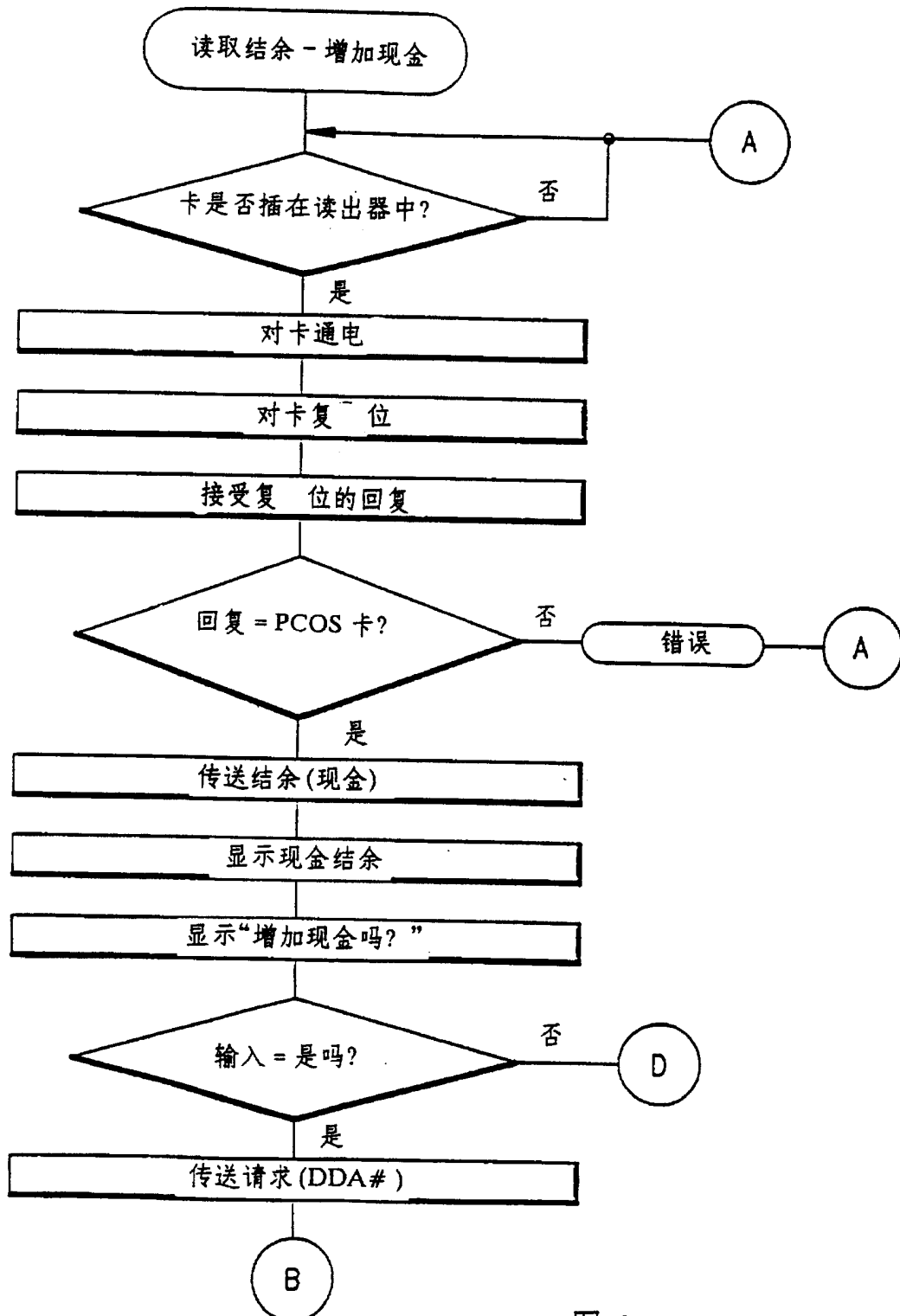


图 6A

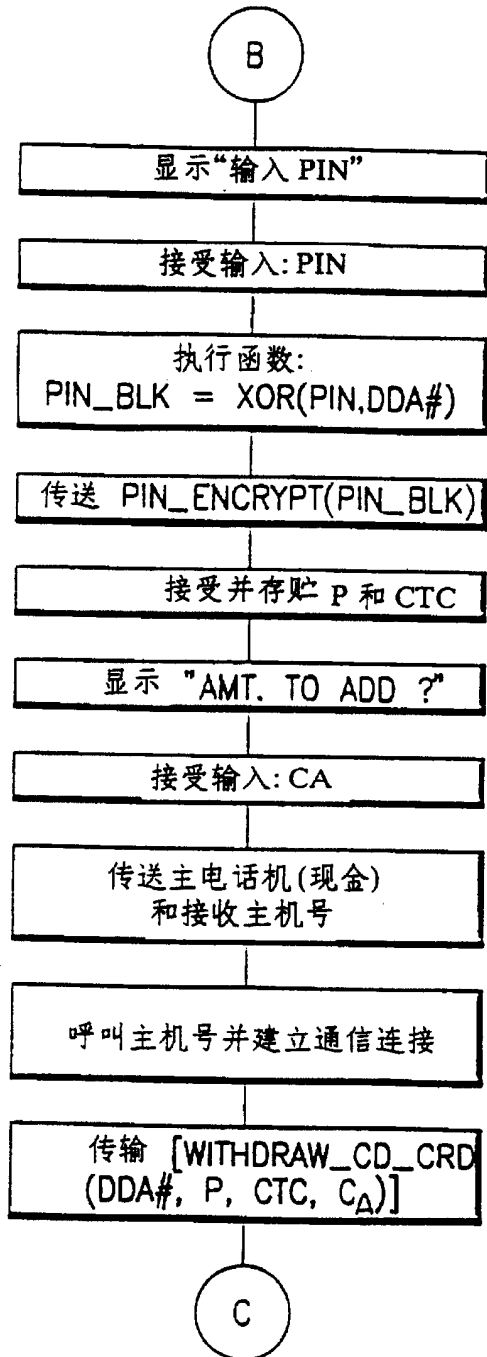


图 6B

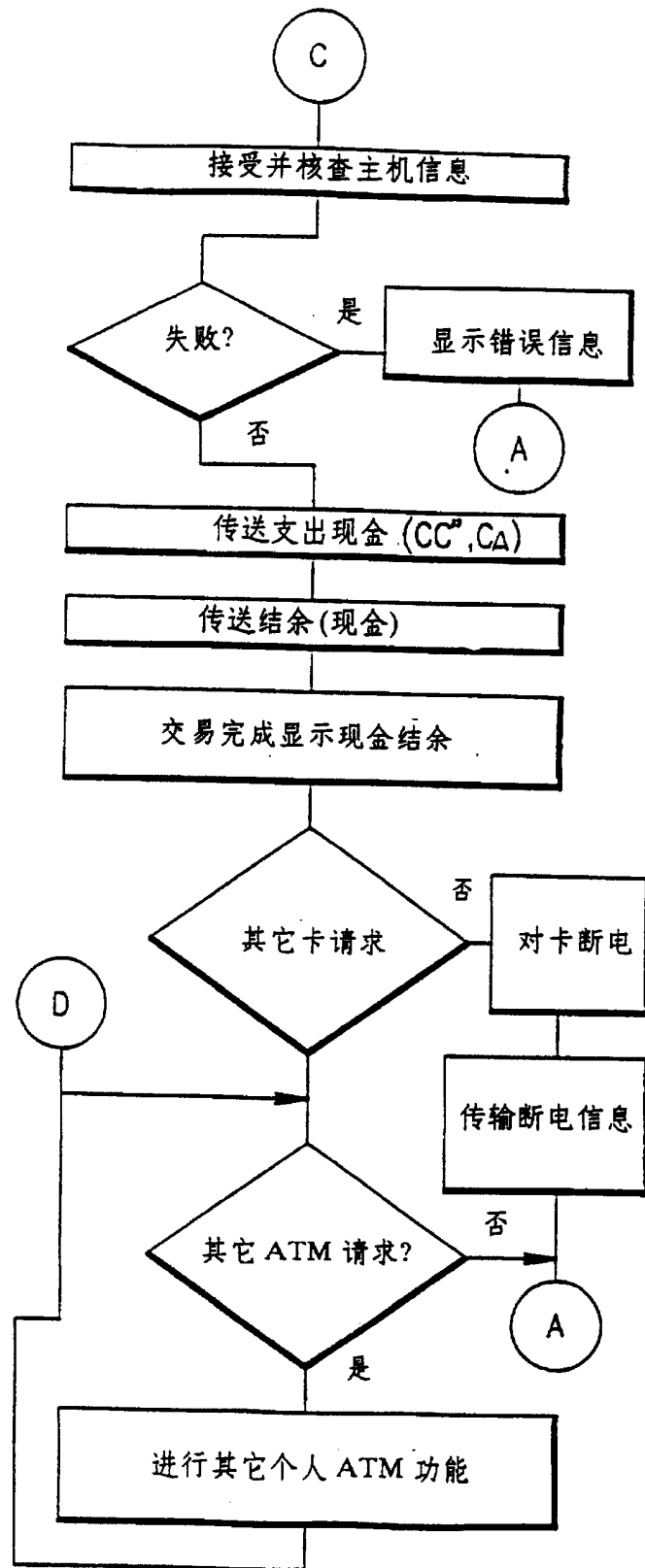


图 6C

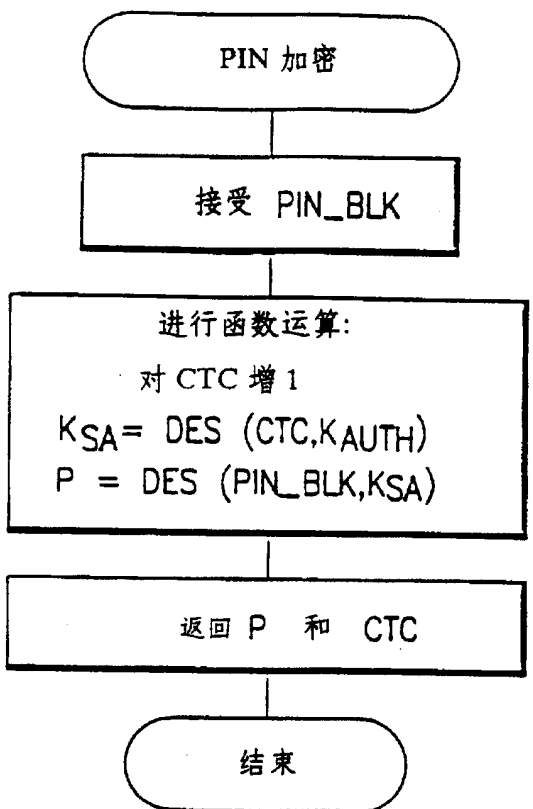


图 7A

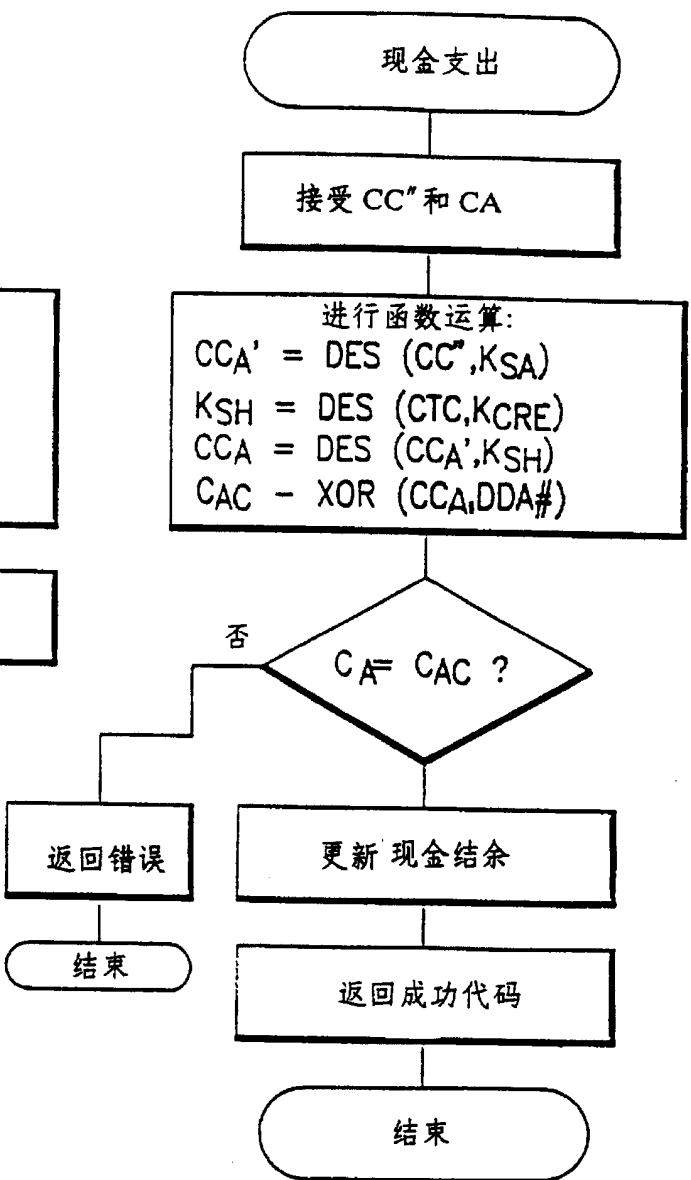


图 7B

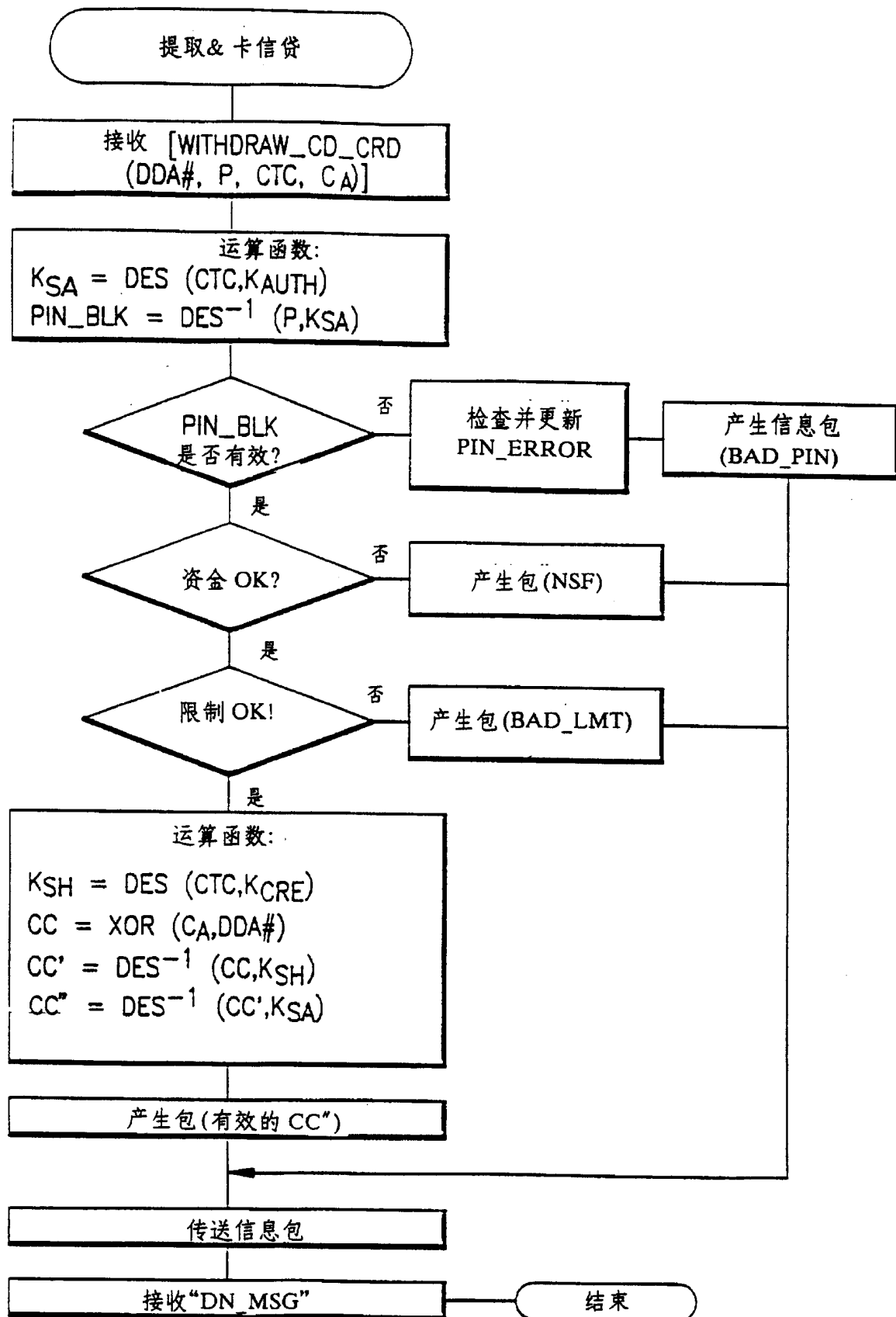


图 8