(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2009 年2 月12 日 (12.02.2009)

PCT

(10) 国际公布号
WO 2009/018683 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2007/002382

(22) 国际申请日: 2007 年8 月8 日 (08.08.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人及
(72) 发明人: **黄金富(WONG, Kamfu)** [CN/CN]; 中国香港特别行政区沙田径口路3号金富台, Hong Kong (CN)。

(74) 代理人: **中国专利代理（香港）有限公司(CHINA PATENT AGENT (H.K.) LTD.)**; 中国香港特别行政区湾仔港湾道23号鹰君中心22号楼, Hong Kong (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告。

(54) Title: A PAYMENT METHOD AND SYSTEM FOR CERTIFICATION BY A SMART CARD WITH A DISPLAY AND A KEYBOARD USING ONE TIME DYNAMIC CIPHER CODE

(54) 发明名称: 带屏幕键盘智能卡用一次性动态密码认证支付方法和系统

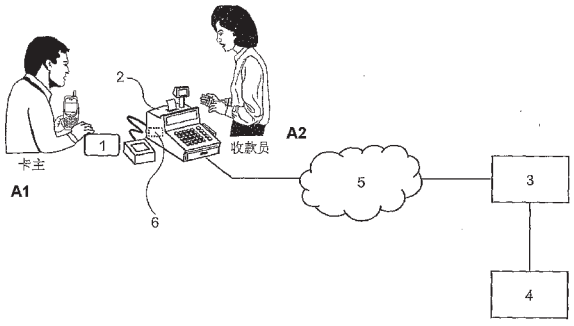

图1 /Fig. 1

A1 card holder
A2 checker

(57) Abstract: A system and method for pay using one time dynamic ciphers and a smart card with a keyboard and a display is provided. The same one cipher code table (7) is set in the smart card (1) and in the account system (4) of the card-issuing bank, respectively, multiple one time ciphers (701) are stored in the cipher code table (7). When paying or transferring accounts, the card holder inputs some information, like account cipher code, money etc., to the smart card (1) in advance, then the smart card (1) extracts an unused one time cipher code (701) from the cipher code table (7) in the card and encrypts the information, and the smart card (1) transmits the encrypted information to the account system (4) of the card-issuing bank through the POS machine (2) and the account system (3) of the card-receiving bank, the account system (4) of the card-issuing bank decrypts the encrypted information using the one time cipher (701) corresponding to the encrypted information. After decrypting, the account system (4) of the card-issuing bank processes the corresponding operations of bank account, like payment, virement and so on, according to the information content.

[见续页]

WO 2009/018683 A1

(57) 摘要：

一种采用一次性动态密码并带有键盘和显示屏智能卡的支付系统和方法，在智能卡（1）和发卡银行帐务系统（4）内分别设有一个相同的密钥表（7），密钥表（7）内储存有多条一次性密钥（701）。当支付或转账时，卡主预先在智能卡（1）上输入账户密码、金额等资料，由智能卡（1）从卡内密钥表（7）提取一条未用的一次性密钥（701）将资料加密，然后智能卡（1）将已加密资料通过 POS 机（2）和收卡银行帐务系统（3）传送到发卡银行帐务系统（4），由发卡银行帐务系统（4）采用与该已加密资料对应的一次性密钥（701）将已加密资料解密，解密成功后发卡银行帐务系统（4）根据资料内容进行相应的支付、转账等银行账户操作。

带屏幕键盘智能卡用一次性动态密码认证支付方法和系统

【技术领域】

本发明涉及使用智能卡进行支付转账的系统和相应方法。

【背景技术】

随着时代的进步，各银行金融机构所发行的各种信用卡、借记卡、付款卡等银行卡也起了很大的变化，从前的银行卡一般都是采用由塑料制成带有磁带的卡，卡上的磁带记录了卡的账户号码等资料，这种带有磁带的银行卡很容易被伪冒复制，各银行金融机构为了增强银行卡的防伪，很多都已经采用了智能卡取代传统的带有磁带的银行卡，这些智能卡一般采用密钥作为防伪保安手段，通过各种加密和解密等措施，使破密需要许多级数以上的资源，令破密变得不可行，保障了智能卡不能被伪冒复制，但随着计算机技术的发展，计算机的运算能力越来越强，一些从前被认为是安全可靠不可破解的防伪保安手段，也可能通过拥有强大运算能力的计算机所破解，令采用这些防伪保安手段的银行卡的安全性受到挑战，为了保障这些智能卡的防伪安全，很多银行金融机构采用了更复杂的防伪保安手段，采用更复杂的密钥和算法的加密解密技术，这样不单会令成本增加，而且随着计算机技术的发展，只要数年时间，在目前被视为安全可靠的防伪保安手段也可能被全面破解，一种能保障银行卡的防伪保安手段，是各银行金融机构所积极研究的问题。

【发明内容】

本发明的目的，在于提供一种具有安全可靠的防伪保安手段的智能卡的支付系统和相应的支付方法，以实现各种大小金额支付转账中的应用。

本发明的目的是这样实现的，采用这样一种带键盘和显示屏智能卡的支付系统，其特征在于，所述的系统包括有智能卡（1）、POS 机（2）、收卡银行帐务系统（3）、发卡银行帐务系统（4）、通讯网络（5）、商户卡（6），其中，收卡银行帐务系统（3）与发卡银行帐务系统（4）相电讯连接，并通过通讯网络（5）与设置于各商户的 POS 机（2）相电讯连接，

以及，

智能卡（1）是带键盘和显示屏的智能卡，主要用于在支付、转账等交易时作为认证卡主的凭证；

POS 机（2）主要用于将交易资料通过通讯网络（5）传送到收卡银行帐务系统（3）进行处理，每一 POS 机（2）内设有一个唯一的 POS 机号（201）；

收卡银行帐务系统（3）主要用于处理交易资料，根据交易资料的内容，通过发卡银行帐务系统（4）对指定的智能卡账户进行相应的转账、支付等银行账户操作；

发卡银行帐务系统（4）主要用于根据收卡银行帐务系统（3）所发出的资料而对指定的智能卡账户进行相应的转账、支付等银行账户操作；

通讯网络（5）可以是有线通讯网络、无线通讯网络、移动电话网络、固网电话网络；

商户卡（6）是一内置于 POS 机（2）的智能卡，主要用于配合 POS 机（2）使用，提供加密、解密、认证、小额支付、找续、充值等功能；

以及，在智能卡（1）和发卡银行帐务系统（4）内分别设有一个相同的密钥表（7），密钥表（7）内储存有多条一次性密钥（701）；当支付或转账时，卡主预先在智能卡（1）上输入账户密码、金额等资料，由智能卡（1）从卡内密钥表（7）提取一条未用的一次性密钥（701）将资料加密，然后智能卡（1）将已加密资料通过 POS 机（2）和收卡银行帐务系统（3）传送到发卡银行帐务系统（4），由发卡银行帐务系统（4）采用与该已加密资料对应的一次性密钥（701）将已加密资料解密，解密成功后发卡银行帐务系统（4）根据资料内容进行相应的支付、转账等银行账户操作。

以及，

所述的智能卡（1）主要结构包括主芯片（101）、键盘（102）、显示装置（103）、通讯接口（104）、电源（105），其中，主芯片（101）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现各项预定功能，包括通过键盘（102）读取卡主输入的资料、通过显示装置（103）显示提示信息、通过通讯接口（104）发送和接收信息、将交易资料加密、储存交易资料、设定密码、上锁、解锁等功能，以及，主芯片（101）内设有一个唯一的卡号（106），以及，智能卡（1）由所述的电源（105）供电运行，所述的电源（105）可以是电池或太阳能电池。

其中，

所述的主芯片（101）内设有一个密钥表（7），密钥表（7）内储存有多条用于验证智能卡（1）身份的一次性密钥（701）和索引号（702），每一索引号（702）对应一条一次性密钥（701）。

以及，

所述的发卡银行帐务系统（4）内设有多个智能卡账户，每一个智能卡账户对应一

智能卡（1），智能卡账户内储存有该账户所对应的智能卡（1）的卡号（106）和一个账户密码，每一个智能卡账户内设有一个密钥表（7），密钥表（7）的内容与该智能卡账户对应的智能卡（1）内的密钥表（7）的内容完全相同，同样储存有多条用于验证智能卡（1）身份的一次性密钥（701）和索引号（702）。

以及，采用这样一种带键盘和显示屏智能卡的支付转账方法，采用前面所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的方法包括卡主预先在智能卡（1）的键盘（102）上输入账户密码、支付金额等交易资料，由智能卡（1）从卡内密钥表（7）提取一条未用的一次性密钥（701）将交易资料加密，然后智能卡（1）将已加密交易资料传送到发卡银行帐务系统（4），由发卡银行帐务系统（4）采用与该已加密交易资料对应的一次性密钥（701）将已加密交易资料解密，解密成功后发卡银行帐务系统（4）根据交易资料内容进行相应的支付、转账等银行账户操作。

在现代密码学里，一次性密钥（One time pad）被认为是不可破解的，密钥只会使用一次，用完即弃，而且密钥是随机产生的，密钥与密钥之间没有关连，保证了密钥的安全。本发明采用了这种一次性密钥作为防伪保安手段，在银行发卡给卡主前，发卡银行预先在发卡银行帐务系统（4）和智能卡（1）内设置一个相同的密钥表（7），密钥表（7）内的每一条一次性密钥（701）只会使用一次，用完即弃，不会重复使用，只要在密钥表（7）设置有足够的一次性密钥（701），例如 5000 条一次性密钥（701），以平均每天用卡支付 5 次计算，5000 条一次性密钥（701）足够卡主使用 1000 天，即大约 3 年时间，如果智能卡（1）的有效期与现时一般的信用卡的有效期一样只有两年，这 5000 条一次性密钥（701）一般都足够卡主在有效期内使用。此外一次性密钥（701）写进智能卡（1）后是不能直接从卡内读出，只能由智能卡（1）内部使用，这可以保障一次性密钥（701）不会被破解，也就保障智能卡（1）不会被伪冒复制。

【附图说明】

图 1 是本发明的带键盘和显示屏智能卡的支付系统结构示意说明图；

图 2 是本发明的智能卡（1）的结构示意说明图；

图 3 是本发明的智能卡（1）的形像化示意图；

图 4 是本发明的另一外型的智能卡（1）的形像化示意图；

图 5 是附有 USB 接口的的智能卡（1）的形像化示意图；

图 6 是本发明的商户卡（6）的结构示意说明图；

图 7 是本发明的带键盘和显示屏智能卡的支付方法第一实施例的步骤示意说明图；

图 8 是本发明的带键盘和显示屏智能卡的支付方法第二实施例的步骤示意说明图；

图 9 是本发明的带键盘和显示屏智能卡的支付方法第三实施例的步骤示意说明图；

图 10 是本发明的带键盘和显示屏智能卡的支付方法第四实施例的步骤示意说明图；

图 11 是本发明的带键盘和显示屏智能卡的支付方法第五实施例的步骤示意说明图；

图 12 是本发明的带键盘和显示屏智能卡的支付方法第六实施例的步骤示意说明图；

图 13 是本发明的带键盘和显示屏智能卡的支付方法第七实施例的步骤示意说明图；

图 14 是本发明的带键盘和显示屏智能卡的支付方法第八实施例的步骤示意说明图；

图 15 是本发明的带键盘和显示屏智能卡的支付方法第九实施例的步骤示意说明图；

图 16 是本发明的带键盘和显示屏智能卡的支付方法第十实施例的步骤示意说明图。

【具体实施方式】

下面结合附图，对本发明的方法作进一步详细说明。图中，相同的数字代表相同的系统、装置、部件器件，方法步骤用圆圈的数字和带箭头的直线所标出。附图是示意性的，用以说明本发明的系统的构成和方法的主要步骤。

参阅图 1，图 1 是本发明的带键盘和显示屏智能卡的支付系统结构示意说明图，图中示出的系统包括有智能卡（1）、POS 机（2）、收卡银行帐务系统（3）、发卡银行帐务系统（4）、通讯网络（5）、商户卡（6），其中，收卡银行帐务系统（3）与发卡银行帐务系统（4）相电讯连接，并通过通讯网络（5）与设置于各商户的 POS 机（2）相电讯连接，

以及，

智能卡（1）是带键盘和显示屏的智能卡，主要用于在支付、转账等交易时作为认证卡主的凭证；

POS 机（2）主要用于将交易资料通过通讯网络（5）传送到收卡银行帐务系统（3）进行处理，以及，POS 机（2）内设有一个唯一的 POS 机号（201）；

收卡银行帐务系统（3）主要用于处理交易资料，根据交易资料的内容，通过发卡银行帐务系统（4）对指定的智能卡账户进行相应的转账、支付等银行账户操作；

发卡银行帐务系统（4）主要用于根据收卡银行帐务系统（3）所发出的资料而对指定的智能卡账户进行相应的转账、支付等银行账户操作；

通讯网络（5）可以是有线通讯网络、无线通讯网络、移动电话网络、固网电话网络；

商户卡（6）是一内置于 POS 机（2）的智能卡，主要用于配合 POS 机（2）使用，

提供加密、解密、认证、小额支付、找续、充值等功能。

以及，

在智能卡（1）和发卡银行帐务系统（4）内分别设有一个相同的密钥表（7），密钥表（7）内储存有多条一次性密钥（701）；当支付或转账时，卡主预先在智能卡（1）上输入账户密码、金额等资料，由智能卡（1）从卡内密钥表（7）提取一条未用的一次性密钥（701）将资料加密，然后智能卡（1）将已加密资料通过 POS 机（2）和收卡银行帐务系统（3）传送到发卡银行帐务系统（4），由发卡银行帐务系统（4）采用与该已加密资料对应的一次性密钥（701）将已加密资料解密，解密成功后发卡银行帐务系统（4）根据资料内容进行相应的支付、转账等银行账户操作。

以及，

所述的发卡银行帐务系统（4）内设有多个智能卡账户，每一个智能卡账户对应一智能卡（1），智能卡账户内储存有该账户所对应的智能卡（1）的卡号（106）和一个账户密码，每一个智能卡账户内设有一个密钥表（7），密钥表（7）的内容与该智能卡账户对应的智能卡（1）内的密钥表（7）的内容完全相同，同样储存有多条用于验证智能卡（1）身份的一次性密钥（701）和索引号（702）。以及，发卡银行帐务系统（4）每次将交易资料加密时，会按预定程序从密钥表(7)内提取一条未用的一次性密钥(701)将交易资料加密，以及，发卡银行帐务系统（4）每次将交易资料解密时，会按预定程序从密钥表（7）内提取一条对应该交易资料的一次性密钥（701）将交易资料解密，以及，发卡银行帐务系统（4）将资料加密或解密后，就会将该条一次性密钥（701）删除或弃置或标记为已用，使该条一次性密钥（701）不会再次被发卡银行帐务系统（4）使用。

所述的收卡银行帐务系统（3）内设有多个商户卡账户，每一个商户卡账户对应一商户卡（6），每一个商户卡账户内设有一个密钥表（8），并储存有该商户卡账户所对应的商户卡（6）的商户卡号（606），密钥表（8）的内容与该商户卡账户对应的商户卡（6）内的密钥表（8）的内容完全相同，同样储存有多条用于验证商户卡（6）身份的一次性密钥（801）和索引号（802）。以及，收卡银行帐务系统（3）每次将交易资料加密时，会按预定程序从密钥表（8）内提取一条未用的一次性密钥（801）将交易资料加密，以及，收卡银行帐务系统（3）每次将交易资料解密时，会按预定程序从密钥表（8）内提取一条对应该交易资料的一次性密钥（801）将交易资料解密，以及，收卡银行帐务系统（3）将资料加密或解密后，就会将该条一次性密钥（801）删除或弃置或标记为已用，使该条一次性密钥（801）不会再次被收卡银行帐务系统（3）使用。

参阅图 2，图 2 是本发明的智能卡（1）的结构示意说明图，图中示出的智能卡（1）主要结构包括主芯片（101）、键盘（102）、显示装置（103）、通讯接口（104）、电源（105），其中，主芯片（101）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现各项预定功能，包括通过键盘（102）读取卡主输入的资料、通过显示装置（103）显示提示信息、通过通讯接口（104）发送和接收信息、将交易资料加密、储存交易资料、设定密码、上锁、解锁等功能，以及，主芯片（101）内设有一个唯一的卡号（106），以及，智能卡（1）由所述的电源（105）供电运行，所述的电源（105）可以是电池或太阳能电池。

其中，

所述的主芯片（101）内设有一个密钥表（7），密钥表（7）内储存有多条用于加密解密和验证智能卡（1）身份的一次性密钥（701）和索引号（702），每一索引号（702）对应一条一次性密钥（701）。

所述的通讯接口（104）可以是无线通讯装置、或有线通讯装置、或蓝芽装置、或红外线装置。

以及，

所述的主芯片（101）每次将交易资料加密时，会按预定程序从密钥表（7）内提取一条未用的一次性密钥（701）将交易资料加密，以及，主芯片（101）每次将交易资料解密时，会按预定程序从密钥表（7）内提取一条对应该交易资料的一次性密钥（701）将交易资料解密，以及，主芯片（101）将交易资料加密或解密后，就会将该条一次性密钥（701）删除或弃置或标记为已用，使该条一次性密钥（701）不会再次被该智能卡（1）使用。

以及，

所述的主芯片（101）还设有开卡口令，每次使用智能卡（1）前，用卡者必须通过键盘（102）输入正确的开卡口令，才能使用智能卡（1）进行各项操作。

参阅图 3 至图 5，图 3 是本发明的智能卡（1）的形像化示意图，图 4 是本发明的另一外型的智能卡（1）的形像化示意图，图 5 是附有 USB 接口的的智能卡（1）的形像化示意图，图 3 至图 5 示出了智能卡（1）以不同实施方式的外形图，图 3 和图 4 中的智能卡（1）附有键盘（102）和显示装置（103），键盘（102）上除了设有数字键外，还设有一般计数机所具备的功能按键，图 5 中的智能卡（1）的通讯接口是 USB 插头，特别适合用于网上支付的用途。

参阅图 6，图 6 是本发明的商户卡（6）的结构示意说明图，图中示出的商户卡（6）

主要结构包括有商户卡芯片（601）、键盘（602）、显示装置（603）、通讯接口（604）、电源（605），其中，商户卡芯片（601）内设有CPU和存储器，并与其它各部件相连接，按预定程序运作，实现各项预定功能，包括通过键盘（602）读取商户卡主输入的资料、通过显示装置（603）显示提示信息、通过通讯接口（604）发送和接收信息、将交易资料加密、储存交易资料、设定密码、上锁、解锁等功能，以及，商户卡芯片（601）内设有一个唯一的卡号（606），以及，商户卡（6）由所述的电源（605）供电运行，所述的电源（605）可以是电池或太阳能电池由POS机（2）供应电源。

其中，

所述的商户卡芯片（601）内设有一个密钥表（8），密钥表（8）内储存有多条用于加密解密和验证商户卡（6）身份的一次性密钥（801）和索引号（802），每一索引号（802）对应一条一次性密钥（801）。

以及，

所述的商户卡芯片（601）每次将交易资料加密时，会按预定程序从密钥表（8）内提取一条未用的一次性密钥（801）将交易资料加密，以及，商户卡芯片（601）每次将交易资料解密时，会按预定程序从密钥表（8）内提取一条对应该交易资料的一次性密钥（801）将交易资料解密，以及，商户卡芯片（601）将交易资料加密或解密后，就会将该条一次性密钥（801）删除或弃置或标记为已用，使该条一次性密钥（801）不会再次被该商户卡（6）使用。

以及，

所述的商户卡芯片（601）设有开卡口令，每次将商户卡（6）插入POS机（2）使用前，必须通过键盘（602）输入正确的开卡口令，商户卡（6）核对开卡口令无误后，就可将商户卡（6）插入POS机（2）使用。

参阅图7，图7是本发明的带键盘和显示屏智能卡的支付方法第一实施例的步骤示意说明图，图中示出的方法包括如下A组步骤，是卡主使用智能卡（1）在商店进行支付时的步骤，具体的步骤如下：

A1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入支付金额和账户密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包A加密成为资料包B，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述

的资料包 A 的内容包括卡号（106）、支付金额、账户密码等资料；

主芯片（101）将资料包 B、卡号（106）和所述的索引号（702）组成资料包 C；

A2. 商店收款员在 POS 机（2）上输入付款金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，智能卡（1）通过通讯接口（104）将在步骤 A1 中所述的资料包 C 传送给 POS 机（2）；

A3. POS 机（2）通过读卡器读取所述的资料包 C 后，将 POS 机号（201）、付款金额、资料包 C 等资料传送到 POS 机（2）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从卡内密钥表（8）内提取一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 D 加密成为资料包 E，加密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；所述的资料包 D 的内容包括商户卡号（606）、POS 机号（201）、付款金额、资料包 C 等资料；

商户卡（6）内的商户卡芯片（601）将资料包 E、商户卡号（606）、索引号（802）等资料组成资料包 F，然后通过通讯接口（104）将所述的资料包 F 传送给 POS 机（2）；

POS 机（2）通过通讯网络（5）将资料包 F 传送到收卡银行帐务系统（3）；

A4. 收卡银行帐务系统（3）从资料包 F 内容中找到资料包 E、商户卡号（606）、索引号（802），从商户卡号（606）找到对应该商户卡号（606）的商户卡账户，从索引号（802）在该商户卡账户的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 E 解密还原出资料包 D，解密成功后表示该资料包 E 是从该商户卡号（606）所对应的商户卡（6）发出的，解密后收卡银行帐务系统（3）从密钥表（8）中将该一次性密钥（801）删除；

收卡银行帐务系统（3）从资料包 D 中找出资料包 C、商户卡号（606）、POS 机号（201）、付款金额等资料，核对该 POS 机号（201）和该商户卡号（606）是否属于同一商户，核对两者属于同一商户无误后，将资料包 C、商户卡号（606）、付款金额等资料传送到发卡银行帐务系统（4）请求转账支付；

A5. 发卡银行帐务系统（4）收到资料包 C、商户卡号（606）、付款金额等资料后，从资料包 C 内容中找到资料包 B、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 B 解密还原出资料包 A，解密成功后表示该资料包 B 是从该卡号（106）所对应的智

能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 A 中找出卡号（106）、支付金额、账户密码等资料，核对支付金额和付款金额相同无误后，发卡银行帐务系统（4）核对账户密码和所述的卡号（106）的智能卡账户结余，核对无误后，从所述的卡号（106）的智能卡账户内转账支付金额的钱到所述的商户卡号（606）在收卡银行帐务系统（3）的商户卡账户；

转账成功后发卡银行帐务系统（4）从所述的智能卡账户的密钥表（7）内提取另一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 1 加密成为资料包 2，加密后发卡银行帐务系统（4）从密钥表（7）中将该另一条一次性密钥（701）删除；所述的资料包 1 的内容包括卡号（106）、商户卡号（606）、已转账支付金额等资料；

发卡银行帐务系统（4）将资料包 2、卡号（106）、该一次性密钥（701）的索引号（702）、商户卡号（606）、已转账支付金额等资料组成资料包 3；

发卡银行帐务系统（4）将资料包 3 传送给收卡银行帐务系统（3）；

A6. 收卡银行帐务系统（3）收到资料包 3 后，从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账支付金额等资料，知道转账成功，将转账支付的交易详细资料储存；

收卡银行帐务系统（3）从所述商户卡号（606）的商户卡账户的密钥表（8）内提取另一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 3 加密成为资料包 4，加密后收卡银行帐务系统（3）从密钥表（8）中将该另一条一次性密钥（801）删除；

收卡银行帐务系统（3）将资料包 4、商户卡号（606）、索引号（802）等资料组成资料包 5；

收卡银行帐务系统（3）将资料包 5 通过通讯网络（5）传送给 POS 机（2）；

A7. POS 机（2）收到资料包 5 后，将资料包 5 传送给 POS 机（2）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从资料包 5 中找到资料包 4、商户卡号（606）、索引号（802）等资料，从索引号（802）在商户卡芯片（601）的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 4 解密还原出资料包 3，解密成功后表示该资料包 4 是由收卡银行帐务系统（3）所发出的，从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、

已转账支付金额等资料，商户卡芯片（601）将该笔交易的资料储存在商户卡芯片（601）内的存储器中，解密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；

商户卡（6）将资料包 3 传送给 POS 机（2）；

POS 机（2）将资料包 3 通过读卡器传送给智能卡（1），并通过 POS 机（2）的显示装置显示已转账支付金额给收款员看，以及打印收条给卡主；

智能卡（1）内的主芯片（101）从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账支付金额等资料，从索引号（702）在主芯片（101）的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 2 解密还原出资料包 1，解密成功后表示该资料包 2 是由发卡银行帐务系统（4）所发出的，主芯片（101）将该笔交易的资料储存在主芯片（101）内的存储器中，解密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；

主芯片（101）从资料包 1 中找到卡号（106）、商户卡号（606）、已转账支付金额等资料，通过显示装置（103）将已转账支付金额显示给卡主看，以及，主芯片（101）自动将智能卡（1）上锁，上锁后的智能卡（1）要输入正确的开卡口令后才能使用。

本实施例中，卡主在刷卡支付前，才通过智能卡（1）上的键盘（102）输入的账户密码，同时智能卡（1）更设有开卡口令，所以即使被贼人盗取了智能卡（1），贼人也无法使用智能卡（1），也盗取不了卡主在发卡银行帐务系统（4）的智能卡账户内的钱。

在本说明书中，为了方便说明，所有有关的加密和解密的过程中，省略了有关加密解密算法的描述，在本发明中，所采用的一次性密钥（701）或一次性密钥（801）进行加密解密时，可以采用一些现有的加密解密算法对资料进行加密解密，例如数据加密标准（DES）、三重数据加密标准（Tri-DES）、RSA、一次性密码（One Time Pad）、公钥基础架构（PKI）等，都可很好实现本发明的目的。此外，在本说明书中，所有有关的加密和解密的过程中，也省略了有关产生校验资料的描述，所述的校验资料是将资料加密前通过校验算法所产生的，然后将资料连同校验资料一同加密，以及，在解密后，通过校验算法就可检测资料和校验资料有没有被窜改过，产生校验资料的校验算法可以采用一些现有的校验资料的算法，例如循环冗余码（CRC）算法、摘要演算法（Message-Digest Algorithm）、消息认证码（Message authentication code）算法、安全杂凑标准（Secure Hash Standard）算法等。在本说明书各实施例的方法步骤中没

有写出这些加密解密算法和校验资料的步骤，是为了方便说明而将这些有关的描述省略，所以在各实施例的方法步骤中的加密解密步骤中，即使没有写出有关加密解密算法和校验资料的步骤，其实都是包含了有关的加密解密算法的步骤和校验资料的步骤。

参阅图 8，图 8 是本发明的带键盘和显示屏智能卡的支付方法第二实施例的步骤示意说明图，图中示出的带键盘和显示屏智能卡的支付系统还包括有 ATM 机（9），ATM 机（9）内设有一个唯一的 ATM 机号（901），以及，ATM 机（9）内置有一商户卡（6）。

本发明的系统除了可应用于商店 POS 机（2）作收付款等支付的应用外，也可用于 ATM 机（9）、网上转账、网上购物支付、手机转账等不同应用，下面以不同的实施例的分别进行详细说明。

继续参阅图 8，图中的第二实施例示出的方法包括如下 B 组步骤，是卡主使用智能卡（1）在 ATM 机（9）进行取款的步骤，具体的步骤如下：

B1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入取款金额和账户密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 A 加密成为资料包 B，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 A 的内容包括卡号（106）、取款金额、账户密码等资料；

主芯片（101）将资料包 B、卡号（106）和所述的索引号（702）组成资料包 C；

B2. 卡主将智能卡（1）放到 ATM 机（9）的读卡器上拍卡，智能卡（1）通过通讯接口（104）将在步骤 A1 中所述的资料包 C 传送给 ATM 机（9）；

B3. ATM 机（9）通过读卡器读取所述的资料包 C 后，将资料包 C 连同 ATM 机号（901）等资料传送到 ATM 机（9）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从卡内密钥表（8）内提取一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 G 加密成为资料包 H，加密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；所述的资料包 G 的内容包括商户卡号（606）、ATM 机号（901）、资料包 C 等资料；

商户卡（6）内的商户卡芯片（601）将资料包 H、商户卡号（606）、索引号（802）组成资料包 J，然后通过通讯接口（104）将所述的资料包 J 传送给 ATM 机（9）；

ATM 机（9）通过通讯网络（5）将资料包 J 传送到收卡银行帐务系统（3）；

B4. 收卡银行帐务系统（3）从资料包 J 内容中找到资料包 H、商户卡号（606）和索引号（802），从商户卡号（606）找到对应该商户卡号（606）的商户卡账户，从索引号（802）在该商户卡账户的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 H 解密还原出资料包 G，解密成功后表示该资料包 H 是从该商户卡号（606）所对应的商户卡（6）发出的，解密后收卡银行帐务系统（3）从密钥表（8）中将该一次性密钥（801）删除；

收卡银行帐务系统（3）从资料包 G 中找出资料包 C、商户卡号（606）、ATM 机号（901）、付款金额等资料，核对该 ATM 机号（901）和该商户卡号（606）是否属于收卡银行的，核对两者属于收卡银行无误后，将资料包 C、商户卡号（606）等资料传送到发卡银行帐务系统（4）请求转账支付；

B5. 发卡银行帐务系统（4）收到资料包 C、商户卡号（606）等资料后，从资料包 C 中找到资料包 B、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 B 解密还原出资料包 A，解密成功后表示该资料包 B 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 A 中找出卡号（106）、取款金额、账户密码等资料，核对取款金额、账户密码和所述的卡号（106）的智能卡账户结余，核对无误后，从所述的卡号（106）的智能卡账户内转账取款金额的钱到所述的商户卡号（606）在收卡银行帐务系统（3）的商户卡账户；

转账成功后发卡银行帐务系统（4）从所述的智能卡账户的密钥表（7）内提取另一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 1 加密成为资料包 2，加密后发卡银行帐务系统（4）从密钥表（7）中将该另一条一次性密钥（701）删除；所述的资料包 1 的内容包括卡号（106）、商户卡号（606）、已转账取款金额等资料；

发卡银行帐务系统（4）将资料包 2、卡号（106）、该一次性密钥（701）的索引号（702）、商户卡号（606）、已转账取款金额等资料组成资料包 3；

发卡银行帐务系统（4）将资料包 3 传送给收卡银行帐务系统（3）；

B6. 收卡银行帐务系统（3）收到资料包 3 后，从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账取款金额等资料，知道转账成功，

将转账支付的交易详细资料储存；

收卡银行帐务系统（3）从所述商户卡号（606）的商户卡账户的密钥表（8）内提取另一条一次性密钥(801)和对应的索引号(802)，以该一次性密钥(801)将资料包 3 加密成为资料包 4，加密后收卡银行帐务系统（3）从密钥表（8）中将该另一条一次性密钥（801）删除；

收卡银行帐务系统（3）将资料包 4、商户卡号（606）、索引号（802）等资料组成资料包 5；

收卡银行帐务系统（3）将资料包 5 通过通讯网络（5）传送给 ATM 机（9）；

B7. ATM 机（9）收到资料包 5 后，将资料包 5 传送给 ATM 机（9）内的商户卡（6）；商户卡(6)内的商户卡芯片(601)从资料包 5 中找到资料包 4、商户卡号(606)、索引号（802）等资料，从索引号（802）在商户卡芯片（601）的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 4 解密还原出资料包 3，解密成功后表示该资料包 4 是由收卡银行帐务系统（3）所发出的，从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账取款金额等资料，商户卡芯片（601）将该笔交易的资料储存在商户卡芯片（601）内的存储器中，解密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；

商户卡（6）将资料包 3 传送给 ATM 机（9）；

ATM 机（9）将资料包 3 通过读卡器传送给智能卡（1），并通过 ATM 机（9）的显示装置显示已转账取款金额给卡主看，以及，ATM 机（9）吐出取款金额的钞票和打印收条给卡主；

智能卡（1）内的主芯片（101）从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账取款金额等资料，从索引号（702）在主芯片（101）的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 2 解密还原出资料包 1，解密成功后表示该资料包 2 是由发卡银行帐务系统（4）所发出的，主芯片（101）将该笔交易的资料储存在主芯片（101）内的存储器中，解密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；

主芯片（101）从资料包 1 中找到卡号（106）、商户卡号（606）、已转账取款金额等资料，通过显示装置（103）将已转账取款金额显示给卡主看，以及，主芯片（101）自动将智能卡（1）上锁，上锁后的智能卡（1）要输入正确的

开卡口令后才能使用。

本实施例中，卡主在ATM机（9）取款前，预先在智能卡（1）输入取款金额和账户密码，然后将智能卡（1）在ATM机（9）上拍卡将取款资料传送给ATM机（9），这样可节省卡主在ATM机（9）上输入密码和取款金额的时间，可减少卡主在ATM机（9）上的操作时间，增加ATM机（9）的效率。

参阅图9，图9是本发明的带键盘和显示屏智能卡的支付方法第三实施例的步骤示意说明图，图中示出的方法包括如下C组步骤，是卡主使用智能卡（1）在网上进行购物时支付的步骤，具体的步骤如下：

C1. 卡主使用可连线上网的电脑终端（12）连线上网，并进入到购物网站（13），根据购物网站（13）内容的引导，选购所需物品，然后在付款时购物网站（13）显示支付金额和购物网站银行账户号码；

卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入支付金额、账户密码、购物网站银行账户号码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包K加密成为资料包L，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包K的内容包括卡号（106）、购物网站银行账户号码、支付金额、账户密码等资料；

主芯片（101）将资料包L、卡号（106）和所述的索引号（702）组成资料包M，并通过显示装置（103）显示给卡主看；

C2. 卡主根据购物网站（13）的网页内容引导，通过电脑终端（12）输入在步骤C1中智能卡（1）所显示的资料包M的内容；

C3. 电脑终端（12）将卡主所输入的资料包M通过互联网络（11）传送到购物网站（13）；

C4. 购物网站（13）将资料包M、购物网站银行账户号码和付款金额等资料组成资料包N，然后将资料包N传送到收卡银行帐务系统（3）；

C5. 收卡银行帐务系统（3）从资料包N中找到资料包M、购物网站银行账户号码、付款金额等资料，从资料包M中找到资料包L、卡号（106）、索引号（702）等资料；

收卡银行帐务系统（3）核对资料无误后，将资料包 M、购物网站银行账户号码、付款金额等资料传送到所述卡号（106）的发卡银行帐务系统（4）请求转账支付；

C6. 发卡银行帐务系统（4）收到资料包 M、购物网站银行账户号码、付款金额等资料后，从资料包 M 内容中找到资料包 L、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 L 解密还原出资料包 K，解密成功后表示该资料包 L 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 K 中找出卡号（106）、购物网站银行账户号码、支付金额、账户密码等资料，核对支付金额和付款金额相同无误后，发卡银行帐务系统（4）核对账户密码和所述的卡号（106）的智能卡账户结余，核对无误后，从所述的卡号（106）的智能卡账户内转账支付金额的钱到收卡银行帐务系统（3）的购物网站银行账户号码的账户内；

C7. 转账后发卡银行帐务系统（4）通知收卡银行帐务系统（3）转账支付成功；

C8. 收卡银行帐务系统（3）通知购物网站（13）转账支付成功；

C9. 购物网站（13）通过互联网络（11）将转账支付成功信息和支付的详细资料传送到电脑终端（12）给卡主看，并安排将卡主所购买的物品送货给卡主。

本实施例中，卡主在支付时，在智能卡（1）输入支付金额、账户密码、购物网站银行账户号码等资料，由智能卡（1）以一次性密钥（701）将交易资料加密，然后通过互联网络（11）传送到购物网站（13），在传送过程中，即使被黑客截取了已加密的交易资料，由于是采用一次性密钥（701）加密，每一次的交易资料是采用不同的一次性密钥（701）加密，黑客也无法凭已加密的交易资料破解出密钥，即使黑客将木马程式入侵到卡主的电脑终端（12）中，由于账户密码是从智能卡（1）上的键盘（102）输入的，并不是在电脑终端（12）上输入，所以黑客采用木马程式入侵方法，也盗取不了卡主的账户密码。

参阅图 10，图 10 是本发明的带键盘和显示屏智能卡的支付方法第四实施例的步骤示意说明图，图中示出的方法包括如下 D 组步骤，是卡主使用智能卡（1）在网上进行转账的步骤，具体的步骤如下：

D1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片

（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入转账金额、账户密码、收款人账户号码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 K 加密成为资料包 L，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 K 的内容包括卡号（106）、收款人账户号码、转账金额、账户密码等资料；

主芯片（101）将资料包 L、卡号（106）和所述的索引号（702）组成资料包 M，并通过显示装置（103）显示给卡主看；

D2. 卡主使用可连线上网的上网终端（12）连线上网，并登入到发卡银行帐务系统（4）的转账网页，根据转账网页内容的引导，通过上网终端（12）输入转账金额、收款人账户号码等资料，以及输入在步骤 D1 中智能卡（1）所显示的资料包 M 的内容；

D3. 上网终端（12）将卡主所输入的资料包 M 通过互联网络（11）传送到发卡银行帐务系统（4）；

D4. 发卡银行帐务系统(4)收到资料包 M 后，从资料包 M 中找到资料包 L、卡号(106)和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 L 解密还原出资料包 K，解密成功后表示该资料包 L 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 K 中找出卡号（106）、收款人账户号码、转账金额、账户密码等资料，核对转账金额、账户密码和所述的卡号（106）的智能卡账户结余及卡主在步骤 D2 中所输入的转账金额、收款人账户号码等资料，核对无误后，从所述的卡号（106）的智能卡账户内转账转账金额的钱到收卡银行帐务系统（3）的收款人账户号码的银行账户内；

D5. 转账后收卡银行帐务系统（3）通知发卡银行帐务系统（4）转账成功；

D6. 发卡银行帐务系统（4）通过互联网络（11）将转账成功信息和转账的详细资料传送到上网终端（12）给卡主看。

参阅图 11，图 11 是本发明的带键盘和显示屏智能卡的支付方法第五实施例的步骤

示意说明图，图中示出的方法包括如下 E 组步骤，是卡主使用智能卡（1）和手机进行转账的步骤，具体的步骤如下：

E1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入转账金额、账户密码、收款人账户号码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 K 加密成为资料包 L，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 K 的内容包括卡号（106）、收款人账户号码、转账金额、账户密码等资料；

主芯片（101）将资料包 L、卡号（106）和所述的索引号（702）组成资料包 M，并通过显示装置（103）显示给卡主看；

E2. 卡主将资料包 M 的内容输入到手机中，然后通过手机和移动电话网络（14）以短信或彩信或 USSD 信息将资料包 M 的内容传送到发卡银行帐务系统（4）；

E3. 发卡银行帐务系统(4)收到资料包 M 后，从资料包 M 中找到资料包 L、卡号(106)和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 L 解密还原出资料包 K，解密成功后表示该资料包 L 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 K 中找出卡号（106）、收款人账户号码、转账金额、账户密码等资料，核对转账金额、账户密码和所述的卡号（106）的智能卡账户结余、收款人账户号码等资料，核对无误后，从所述的卡号（106）的智能卡账户内转账转账金额的钱到收卡银行帐务系统（3）的收款人账户号码的银行账户内；

E4. 转账后收卡银行帐务系统（3）通知发卡银行帐务系统（4）转账成功；

E5. 发卡银行帐务系统（4）通过移动电话网络（14）以短信或彩信或 USSD 信息将转账成功信息和转账的详细资料传送到卡主手机给卡主看。

第四和第五实施例中，采用了不同的方法进行转账，都是预先在智能卡（1）上输入转账资料，然后由智能卡（1）以一次性密钥（701）将转账资料加密，然后通过不同

的途径传送到发卡银行帐务系统（4），包括通过互联网络（11）、短信、彩信、USSD信息等方式传送，由于转账资料已经加密，卡主的账户密码不会在传送途径中泄露，所以对传送的途径的安全要求不高，与现时一般网上银行技术相比，本发明的转账支付方法更安全可靠。

参阅图 12，图 12 是本发明的带键盘和显示屏智能卡的支付方法第六实施例的步骤示意说明图，图中示出的方法包括如下 F 组步骤，是卡主使用智能卡（1）和手机进行转账的步骤，具体的步骤如下：

F1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入转账金额、账户密码、收款人手机电话号码、接收款项密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 0 加密成为资料包 P，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 0 的内容包括卡号（106）、收款人手机电话号码、接收款项密码、转账金额、账户密码等资料；

主芯片（101）将资料包 P、卡号（106）和所述的索引号（702）组成资料包 Q，并通过显示装置（103）显示给卡主看；

F2. 卡主将资料包 Q 的内容输入到手机中，然后通过手机和移动电话网络（14）以短信或彩信或 USSD 信息将资料包 Q 传送到发卡银行帐务系统（4）；

F3. 发卡银行帐务系统(4)收到资料包 Q 后，从资料包 Q 中找到资料包 P、卡号(106)和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 P 解密还原出资料包 0，解密成功后表示该资料包 P 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 0 中找出卡号（106）、收款人手机电话号码、接收款项密码、转账金额、账户密码等资料，核对转账金额、账户密码和所述的卡号（106）的智能卡账户结余等资料，核对无误后，从所述的卡号（106）的智能卡账户内暂时冻结转账金额的钱，等待收款人在指定时间内凭接收款项密码提取该笔款项，例如在 5 分钟内；

发卡银行帐务系统（4）通过移动电话网络（14）发短信或彩信或USSD信息给卡主手机，通知卡主已经准备妥该笔转账款项，收款人可在指定时间内凭接收款项密码提取该笔款项；

F4. 收款人在指定时间内用自己的收款人手机通过移动电话网络（14）以短信或彩信或USSD信息将接收转账款项信息传送到发卡银行帐务系统（4），所述的接收转账款项信息包括收款人在收卡银行帐务系统（3）的收款人账户号码和接收款项密码；

F5. 发卡银行帐务系统（4）收到接收转账款项信息后，从接收转账款项信息的来源电话号码找到收款人手机电话号码，从收款人手机电话号码在发卡银行帐务系统（4）中找到在步骤F3中所述的暂时冻结转账转账金额的钱的记录，从接收转账款项信息内容找到收款人账户号码和接收款项密码，核对该信息内的接收款项密码与所述的暂时冻结转账金额的钱的记录中的接收款项密码相同无误后，发卡银行帐务系统（4）将该笔暂时冻结转账金额的钱转账到收卡银行帐务系统（3）内的收款人账户号码的账户；

F6. 转账后收卡银行帐务系统（3）通知发卡银行帐务系统（4）转账成功；

F7. 发卡银行帐务系统（4）通过通过移动电话网络（14）发短信或彩信或USSD信息给收款人手机，通知收款人已经成功接收转账款项及转账金额；

F8. 发卡银行帐务系统（4）通过通过移动电话网络（14）发短信或彩信或USSD信息给卡主手机，通知卡主收款人已经成功接收该笔转账款项和转账金额。

本实施例中，只要卡主知道收款人的手机电话号码，就可以进行转账，卡主无须将自己的账户号码泄露给收款人知，而收款人也可因应自己的需要，将转账的钱提取存到自己指定的银行账户内，整个过程都不会泄露双方的银行账户号码，可保障双方的私隐。

参阅图13，图13是本发明的带键盘和显示屏智能卡的支付方法第七实施例的步骤示意说明图，图中示出的方法包括如下G组步骤，是卡主使用智能卡（1）和手机进行遥距ATM取款的步骤，具体的步骤如下：

G1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入取款金额、账户密码、接收款项密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包R加密成为资料包

S，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 R 的内容包括卡号（106）、接收款项密码、取款金额、账户密码等资料；

主芯片（101）将资料包 S、卡号（106）和所述的索引号（702）组成资料包 T，并通过显示装置（103）显示给卡主看；

G2. 卡主将资料包 T 的内容输入到手机中，然后通过手机和移动电话网络（14）以短信或彩信或 USSD 信息将资料包 T 的内容传送到发卡银行帐务系统（4）；

G3. 发卡银行帐务系统（4）收到资料包 T 的内容的信息后，从信息内容中找到资料包 S、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 S 解密还原出资料包 R，解密成功后表示该资料包 S 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 R 中找出卡号（106）、接收款项密码、取款金额、账户密码等资料，核对取款金额、账户密码和所述的卡号（106）的智能卡账户结余等资料，核对无误后，从所述的卡号（106）的智能卡账户内暂时冻结取款金额的钱，等待取款人在指定时间内凭接收款项密码提取该笔款项，例如在 5 分钟内，如果取款人在指定时间过后仍未成功提取该笔款项，发卡银行帐务系统（4）会将该笔款项解冻退回所述的智能卡账户内；

发卡银行帐务系统（4）通过移动电话网络（14）发短信或彩信或 USSD 信息给卡主手机，通知卡主已经准备妥该笔取款款项，取款人可在指定时间内到 ATM 机（9）凭接收款项密码提取该笔款项；

G4. 取款人在指定时间内走到 ATM 机（9）前，在 ATM 机（9）输入卡主的卡号（106）、提款金额、接收款项密码等资料；

G5. ATM 机（9）将卡号（106）、ATM 机号（901）、提款金额、接收款项密码等资料传送到 ATM 机（9）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从卡内密钥表（8）内提取一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 U 加密成为资料包 V，加密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；所述的资料包 U 的内容包括有卡号（106）、提款金额、接收款项密码、商户卡号（606）、ATM 机号（901）等资料；

商户卡（6）内的商户卡芯片（601）将资料包 V、商户卡号（606）、索引号（802）组成资料包 W，然后通过通讯接口（104）将资料包 W 传送给 ATM 机（9）；

ATM 机（9）通过通讯网络（5）将资料包 W 传送到收卡银行帐务系统（3）；

G6. 收卡银行帐务系统（3）从资料包 W 中找到资料包 V、商户卡号（606）和索引号（802），从商户卡号（606）找到对应该商户卡号（606）的商户卡账户，从索引号（802）在该商户卡账户的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 V 解密还原出资料包 U，解密成功后表示该资料包 V 是从该商户卡号（606）所对应的商户卡（6）发出的，解密后收卡银行帐务系统（3）从密钥表（8）中将该一次性密钥（801）删除；

收卡银行帐务系统（3）从资料包 U 中找出卡号（106）、提款金额、接收款项密码、商户卡号（606）、ATM 机号（901）等资料，核对该 ATM 机号（901）和该商户卡号（606）是否属于收卡银行的，核对两者属于收卡银行无误后，将卡号（106）、提款金额、接收款项密码、商户卡号（606）等资料传送到发卡银行帐务系统（4）请求转账支付；

G7. 发卡银行帐务系统（4）收到卡号（106）、提款金额、接收款项密码、商户卡号（606）等资料后，从卡号（106）在发卡银行帐务系统（4）中找到在步骤 G3 中所述的暂时冻结取款金额的钱的记录，核对接收款项密码与所述的暂时冻结取款金额的钱的记录中的接收款项密码是否相同，并核对提款金额与所述的暂时冻结取款金额的钱的记录中的取款金额是否相同，核对两者相同无误后，发卡银行帐务系统（4）将该笔暂时冻结取款金额的钱转账到所述的商户卡号（606）在收卡银行帐务系统（3）的商户卡账户内，并通知收卡银行帐务系统（3）转账成功；

G8. 收卡银行帐务系统（3）收到转账成功通知后，收卡银行帐务系统（3）从所述商户卡号（606）的商户卡账户的密钥表（8）内提取另一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 6 加密成为资料包 7，加密后收卡银行帐务系统（3）从密钥表（8）中将该另一条一次性密钥（801）删除，所述的资料包 6 的内容包括卡号（106）、提款金额、商户卡号（606）、ATM 机号（901）等资料；

收卡银行帐务系统（3）将资料包 7、商户卡号（606）、索引号（802）等组成资料包 8；

收卡银行帐务系统（3）将资料包 8 通过通讯网络（5）传送给 ATM 机（9）；

G9. ATM 机（9）收到资料包 8 后，将资料包 8 传送给 ATM 机（9）内的商户卡（6）；商户卡(6)内的商户卡芯片(601)从资料包 8 中找到资料包 7、商户卡号(606)、索引号（802）等资料，从索引号（802）在商户卡芯片（601）的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 7 解密还原出资料包 6，解密成功后表示该资料包 7 是由收卡银行帐务系统（3）所发出的，从资料包 6 中找到卡号（106）、提款金额、商户卡号（606）、ATM 机号（901）等资料，商户卡芯片（601）将该笔提款操作的资料储存在商户卡芯片（601）内的存储器中，解密后商户卡芯片(601)从密钥表(8)中将该一次性密钥(801)删除；

商户卡（6）将资料包 6 传送给 ATM 机（9）；

ATM 机（9）收到资料包 6 后，通过 ATM 机（9）的显示装置显示提款成功信息及提款金额给取款人看，以及，ATM 机（9）吐出提款金额的钞票和打印收条给取款人；

G10. 发卡银行帐务系统（4）通过移动电话网络（14）发短信或彩信或 USSD 信息给卡主手机，通知卡主取款人已经在指定时间内到 ATM 机（9）提取该笔款项。

本实施例中，卡主可以请他人代自己到 ATM 机（9）取款而不会泄露卡主的银行账户密码。

以上各实施例已经详细说明了本发明的系统和支付转账方法，由于本发明的智能卡（1）上设置了键盘（102），而账户密码等交易资料都是预先在智能卡（1）上输入，这样等于将原来在 POS 机（2）、ATM 机（9）、上网终端（12）等交易终端上的键盘搬到智能卡（1）上，是一种将键盘私有化的智能卡系统，由于输入账户密码的键盘和交易终端的分离，使账户密码的安全得到了充分的保障，以后 POS 机（2）、ATM 机（9）上甚至可以无须设置密码键盘，所有原来在密码键盘上的操作都可由智能卡（1）上的键盘（102）进行。

本发明的更进一步改进是增加小金额支付功能，小金额支付时钱是直接从智能卡（1）内扣钱存到 POS 机（2）内的商户卡（6），和以上各实施例的支付方法相比，小金额支付时 POS 机（2）无须连线到收卡银行帐务系统（3），可节省通讯费用和加快整个支付过程所需时间。本进一步改进的实现方法是在智能卡（1）和商户卡（6）增设用于储存小金额支付记录的多个存储区，包括在智能卡（1）的主芯片（101）内设有多个存储区，包括小额存入区、小额支出区、充值记录区、结余记录区、其他用途区，

其中，

小额存入区主要用于储存小额存入记录；

小额支出区主要用于储存小额支出记录；

充值记录区主要用于储存充值记录；

结余记录区主要用于储存结余记录；

其他用途区用于其他用途；

以及，

主芯片（101）内储存有预定加密算法 A 和预定加密算法 B，通过预定加密算法 A 和预定加密算法 B 对小额存入区、小额支出区、充值记录区、结余记录区等存储区内的内容进行加密和解密等保护措施；

以及，

主芯片（101）内储存有一个小额支付上限金额，所有写入小额存入区或小额支出区的每一笔记录中的存入或支出金额不能超过所述的小额支付上限金额。

在商户卡（6）方面，商户卡（6）的商户卡芯片（601）内设有多个存储区，包括收款记录区、支出记录区、充值记录区、结余记录区、其他用途区，

其中，

收款记录区主要用于储存小额存入记录；

支出记录区主要用于储存小额支出记录；

充值记录区主要用于储存充值记录；

结余记录区主要用于储存结余记录；

其他用途区用于其他用途；

以及，

商户卡芯片（601）内储存有预定加密算法 A 和预定加密算法 B，通过预定加密算法 A 和预定加密算法 B 对收款记录区、支出记录区、充值记录区、结余记录区等存储区内的内容进行加密和解密等保护措施；

以及，

商户卡芯片（601）内储存有一个交易上限金额，所有写入收款记录区或支出记录区的每一笔记录中的存入或支出金额不能超过所述的交易上限金额。

此外，采用这样一种带键盘和显示屏智能卡的小金额交易支付方法，其特征在于，所述的方法包括在支付时，通过 POS 机（2）从智能卡（1）内结余记录区所储存的结余金额转移与支付金额相等的部份结余到商户卡（6）内结余记录区所储存的结余金额内，以及，在找续或充值时，通过 POS 机（2）从商户卡（6）内结余记录区所储存的结余金

额转移与支付金额相等的部份结余到智能卡（1）内结余记录区所储存的结余金额内。

参阅图 14，图 14 是本发明的带键盘和显示屏智能卡的支付方法第八实施例的步骤示意说明图，图中示出的方法包括如下 H 组步骤，是卡主使用智能卡（1）在商店进行小金额支付时的步骤，具体的步骤如下：

H1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1）；

H2. 商店收款员在 POS 机（2）上输入支付金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，POS 机（2）读取智能卡（1）的卡号（106）成功后，POS 机（2）将卡号（106）、POS 机号（201）、支付金额等资料传送到 POS 机（2）内的商户卡（6），商户卡（6）内的商户卡芯片（601）以预定的加密算法 B 将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等支付资料加密后传送回 POS 机（2），由 POS 机（2）将已加密支付资料通过读卡器传送给智能卡（1）；

H3. 智能卡（1）通过通讯接口（104）收到已加密支付资料，以预定的加密算法 B 将已加密支付资料解密还原出卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等资料，核对卡号（106）和支付金额少于小额支付上限金额无误后，智能卡（1）内的主芯片（101）从结余记录区内读取最新的一笔结余记录，并核对所述的结余记录内的结余金额不少于支付金额，核对无误后将结余金额减去支付金额计算出新的结余金额，然后将新的结余金额写进结余记录区内和将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等资料写进小额支出区内，并以预定的加密算法 A 将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等小额交易资料加密，通过通讯接口（104）传送给 POS 机（2），并通过显示装置（103）显示支付金额和最新结余给卡主看，以及，主芯片（101）自动将智能卡（1）上锁，上锁后的智能卡（1）要输入正确的开卡口令后才能使用；

H4. POS 机（2）通过读卡器读取所述的已加密小额交易资料后，将已加密小额交易资料传送到 POS 机（2）内的商户卡（6），商户卡（6）内的主芯片（101）以预定的加密算法 A 将已加密小额交易资料解密，解密成功后还原出卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等小额交易资料，核对资料无误后将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等资料写

进收款记录区内，并从结余记录区内读取最新的一笔结余记录，将所述的结余记录内的结余金额加上支付金额计算出新的结余金额，然后将新的结余金额写进结余记录区内，以及，商户卡（6）向 POS 机（2）发出支付成功信息；

H5. POS 机（2）收到支付成功信息后，立即打印收条给卡主，小额支付操作完成。

参阅图 15，图 15 是本发明的带键盘和显示屏智能卡的支付方法第九实施例的步骤示意说明图，图中示出的方法包括如下 J 组步骤，是卡主使用现钞付款，商户将找续零钱存入卡主的智能卡（1）的步骤，具体的步骤如下：

J1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1）；

J2. 卡主以现钞付款后，商店收款员在 POS 机（2）上输入支付金额和现钞金额后，POS 机（2）计算出找续金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，POS 机（2）读取智能卡（1）的卡号（106）成功后，POS 机（2）将卡号（106）和找续金额传送给 POS 机（2）内的商户卡（6），商户卡（6）核对找续金额少于小额支付上限金额后，商户卡（6）内的商户卡芯片（601）从结余记录区内读取最新的一笔结余记录，并核对所述的结余记录内的结余金额不少于找续金额，核对无误后将结余金额减去找续金额计算出新的结余金额，然后将新的结余金额写进结余记录区内和将卡号（106）、商户卡号（606）、POS 机号（201）、找续金额等资料写进支出记录区内，并以预定的加密算法 B 将卡号（106）、商户卡号（606）、POS 机号（201）、找续金额等小额找续资料加密，通过通讯接口（604）传送给 POS 机（2）；

J3. POS 机（2）通过读卡器所述的已加密小额找续资料传送给智能卡（1），智能卡（1）内的主芯片（101）以预定的加密算法 B 将已加密小额找续资料解密，解密成功后还原出卡号（106）、商户卡号（606）、POS 机号（201）、找续金额等小额找续资料，核对资料无误后将卡号（106）、商户卡号（606）、POS 机号（201）、找续金额写进小额存入区内，并从结余记录区内读取最新的一笔结余记录，将所述的结余记录内的结余金额加上找续金额计算出新的结余金额，然后将新的结余金额写进结余记录区内，以及，通过显示装置（103）显示找续金额和最新结余，并向 POS 机（2）发出找续成功信息；

J4. POS 机（2）收到找续成功信息后，立即打印收条给卡主，小额找续操作完成。

参阅图 16，图 16 是本发明的带键盘和显示屏智能卡的支付方法第十实施例的步骤

示意说明图，图中示出的方法包括如下K组步骤，是卡主在商户使用现钞付款充值智能卡（1）的步骤，具体的步骤如下：

K1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1）；

K2. 卡主将充值金额的现钞交给商户的收款员，商店收款员点收现钞后在POS机(2)上输入充值金额，然后卡主将智能卡（1）放到POS机（2）的读卡器上拍卡，POS机（2）读取智能卡（1）的卡号（106）成功后，POS机（2）将卡号（106）和充值金额传送给POS机（2）内的商户卡（6），商户卡（6）核对充值金额少于小额支付上限金额后，商户卡（6）内的商户卡芯片（601）从结余记录区内读取最新的一笔结余记录，并核对所述的结余记录内的结余金额不少于充值金额，核对无误后将结余金额减去充值金额计算出新的结余金额，然后将新的结余金额写进结余记录区内和将卡号(106)、商户卡号(606)、POS机号(201)、充值金额等资料写进支出记录区内，并以预定的加密算法B将卡号（106）、商户卡号（606）、POS机号（201）、充值金额等充值资料加密，通过通讯接口（604）传送给POS机（2）；

K3. POS机（2）通过读卡器所述的已加密充值资料传送给智能卡（1），智能卡（1）内的主芯片（101）以预定的加密算法B将已加密充值资料解密，解密成功后还原出卡号（106）、商户卡号（606）、POS机号（201）、充值金额等充值资料，核对资料无误后将卡号（106）、商户卡号（606）、POS机号（201）、充值金额写进充值记录区内，并从结余记录区内读取最新的一笔结余记录，将所述的结余记录内的结余金额加上充值金额计算出新的结余金额，然后将新的结余金额写进结余记录区内，以及，通过显示装置（103）显示充值金额和最新结余，并向POS机（2）发出充值成功信息；

K4. POS机（2）收到充值成功信息后，立即打印收条给卡主，充值操作完成。

本发明的带键盘和显示屏智能卡的支付系统和支付转账方法，采用现代密码学里被认为是不可破解的一次性密钥，安全可靠，成本低廉，它的实施，会带来良好的社会效益和经济效益，对银行和顾客都十分裨益。

权利要求

1. 一种带键盘和显示屏智能卡的支付系统，其特征在于，所述的系统包括有智能卡（1）、POS 机（2）、收卡银行帐务系统（3）、发卡银行帐务系统（4）、通讯网络（5）、商户卡（6），其中，收卡银行帐务系统（3）与发卡银行帐务系统（4）相电讯连接，并通过通讯网络（5）与设置于各商户的 POS 机（2）相电讯连接，

以及，

智能卡（1）是带键盘和显示屏的智能卡，主要用于在支付、转账等交易时作为认证卡主的凭证；

POS 机（2）主要用于将交易资料通过通讯网络（5）传送到收卡银行帐务系统（3）进行处理，每一 POS 机（2）内设有一个唯一的 POS 机号（201）；

收卡银行帐务系统（3）主要用于处理交易资料，根据交易资料的内容，通过发卡银行帐务系统（4）对指定的智能卡账户进行相应的转账、支付等银行账户操作；

发卡银行帐务系统（4）主要用于根据收卡银行帐务系统（3）所发出的资料而对指定的智能卡账户进行相应的转账、支付等银行账户操作；

通讯网络（5）可以是有线通讯网络、无线通讯网络、移动电话网络、固网电话网络；

商户卡（6）是一内置于 POS 机（2）的智能卡，主要用于配合 POS 机（2）使用，提供加密、解密、认证、小额支付、找续、充值等功能；

以及，

在智能卡（1）和发卡银行帐务系统（4）内分别设有一个相同的密钥表（7），密钥表（7）内储存有多条一次性密钥（701）；当支付或转账时，卡主预先在智能卡（1）上输入账户密码、金额等资料，由智能卡（1）从卡内密钥表（7）提取一条未用的一次性密钥（701）将资料加密，然后智能卡（1）将已加密资料通过 POS 机（2）和收卡银行帐务系统（3）传送到发卡银行帐务系统（4），由发卡银行帐务系统（4）采用与该已加密资料对应的一次性密钥（701）将已加密资料解密，解密成功后发卡银行帐务系统（4）根据资料内容进行相应的支付、转账等银行账户操作。

2. 如权利要求 1 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的智能卡（1）主要结构包括主芯片（101）、键盘（102）、显示装置（103）、通讯接口

（104）、电源（105），其中，主芯片（101）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现各项预定功能，包括通过键盘（102）读取卡主输入的资料、通过显示装置（103）显示提示信息、通过通讯接口（104）发送和接收信息、将交易资料加密、储存交易资料、设定密码、上锁、解锁等功能，以及，主芯片（101）内设有一个唯一的卡号（106），以及，智能卡（1）由所述的电源（105）供电运行，所述的电源（105）可以是电池或太阳能电池。

3. 如权利要求 2 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的主芯片（101）内设有一个密钥表（7），密钥表（7）内储存有多条用于加密解密和验证智能卡（1）身份的一次性密钥（701）和索引号（702），每一索引号（702）对应一条一次性密钥（701）。

4. 如权利要求 3 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的主芯片（101）每次将交易资料加密时，会按预定程序从密钥表（7）内提取一条未用的一次性密钥（701）将交易资料加密，以及，主芯片（101）每次将交易资料解密时，会按预定程序从密钥表（7）内提取一条对应该交易资料的一次性密钥（701）将交易资料解密，以及，主芯片（101）将交易资料加密或解密后，就会将该条一次性密钥（701）删除或弃置或标记为已用，使该条一次性密钥（701）不会再次被该智能卡（1）使用。

5. 如权利要求 2 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的主芯片（101）还设有开卡口令，每次使用智能卡（1）前，用卡者必须通过键盘（102）输入正确的开卡口令，才能使用智能卡（1）进行各项操作。

6. 如权利要求 2 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的通讯接口（104）可以是无线通讯装置、或有线通讯装置、或蓝芽装置、或红外线装置。

7. 如权利要求 2 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的主芯片（101）内设有多个存储区，包括小额存入区、小额支出区、充值记录区、结余记录区、其他用途区，
其中，

小额存入区主要用于储存小额存入记录；
小额支出区主要用于储存小额支出记录；
充值记录区主要用于储存充值记录；
结余记录区主要用于储存结余记录；
其他用途区用于其他用途；
以及，
主芯片（101）内储存有预定加密算法 A 和预定加密算法 B，通过预定加密算法 A 和预定加密算法 B 对小额存入区、小额支出区、充值记录区、结余记录区等存储区内的内容进行加密和解密等保护措施；
以及，
主芯片（101）内储存有一个小额支付上限金额，所有写入小额存入区或小额支出区的每一笔记录中的存入或支出金额不能超过所述的小额支付上限金额。

8. 如权利要求 1 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的商户卡（6）主要结构包括有商户卡芯片（601）、键盘（602）、显示装置（603）、通讯接口（604）、电源（605），其中，商户卡芯片（601）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现各项预定功能，包括通过键盘（602）读取商户卡主输入的资料、通过显示装置（603）显示提示信息、通过通讯接口（604）发送和接收信息、将交易资料加密、储存交易资料、设定密码、上锁、解锁等功能，以及，商户卡芯片（601）内设有一个唯一的卡号（606），以及，商户卡（6）由所述的电源（605）供电运行，所述的电源（605）可以是电池或太阳能电池由 POS 机（2）供应电源。

9. 如权利要求 8 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的商户卡芯片（601）内设有一个密钥表（8），密钥表（8）内储存有多条用于加密解密和验证商户卡（6）身份的一次性密钥（801）和索引号（802），每一索引号（802）对应一条一次性密钥（801）。

10. 如权利要求 9 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的商户卡芯片（601）每次将交易资料加密时，会按预定程序从密钥表（8）内提取一条未用的一次性密钥（801）将交易资料加密，以及，商户卡芯片（601）每次将交易资

料解密时，会按预定程序从密钥表（8）内提取一条对应该交易资料的一次性密钥（801）将交易资料解密，以及，商户卡芯片（601）将交易资料加密或解密后，就会将该条一次性密钥（801）删除或弃置或标记为已用，使该条一次性密钥（801）不会再次被该商户卡（6）使用。

11. 如权利要求 8 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的商户卡芯片（601）设有开卡口令，每次将商户卡（6）插入 POS 机（2）使用前，必须通过键盘（602）输入正确的开卡口令，商户卡（6）核对开卡口令无误后，就可将商户卡（6）插入 POS 机（2）使用。

12. 如权利要求 8 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的商户卡芯片（601）内设有多个存储区，包括收款记录区、支出记录区、充值记录区、结余记录区、其他用途区，

其中，

收款记录区主要用于储存小额存入记录；

支出记录区主要用于储存小额支出记录；

充值记录区主要用于储存充值记录；

结余记录区主要用于储存结余记录；

其他用途区用于其他用途；

以及，

商户卡芯片（601）内储存有预定加密算法 A 和预定加密算法 B，通过预定加密算法 A 和预定加密算法 B 对收款记录区、支出记录区、充值记录区、结余记录区等存储区内的内容进行加密和解密等保护措施；

以及，

商户卡芯片（601）内储存有一个交易上限金额，所有写入收款记录区或支出记录区的每一笔记录中的存入或支出金额不能超过所述的交易上限金额。

13. 如权利要求 1 或 2 或 3 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的发卡银行帐务系统（4）内设有多个智能卡账户，每一个智能卡账户对应一智能卡（1），智能卡账户内储存有该账户所对应的智能卡（1）的卡号（106）和一个账户密码，每一个智能卡账户内设有一个密钥表（7），密钥表（7）的内容与该

智能卡账户对应的智能卡（1）内的密钥表（7）的内容完全相同，同样储存有多条用于验证智能卡（1）身份的一次性密钥（701）和索引号（702）。

14. 如权利要求 1 或 8 或 9 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的收卡银行帐务系统（3）内设有多个商户卡账户，每一个商户卡账户对应一商户卡（6），每一个商户卡账户内设有一个密钥表（8），并储存有该商户卡账户所对应的商户卡（6）的商户卡号（606），密钥表（8）的内容与该商户卡账户对应的商户卡（6）内的密钥表（8）的内容完全相同，同样储存有多条用于验证商户卡（6）身份的一次性密钥（801）和索引号（802）。

15. 如权利要求 13 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的发卡银行帐务系统（4）每次将交易资料加密时，会按预定程序从密钥表（7）内提取一条未用的一次性密钥（701）将交易资料加密，以及，发卡银行帐务系统（4）每次将交易资料解密时，会按预定程序从密钥表（7）内提取一条对应该交易资料的一次性密钥（701）将交易资料解密，以及，发卡银行帐务系统（4）将资料加密或解密后，就会将该条一次性密钥（701）删除或弃置或标记为已用，使该条一次性密钥（701）不会再次被发卡银行帐务系统（4）使用。

16. 如权利要求 14 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的收卡银行帐务系统（3）每次将交易资料加密时，会按预定程序从密钥表（8）内提取一条未用的一次性密钥（801）将交易资料加密，以及，收卡银行帐务系统（3）每次将交易资料解密时，会按预定程序从密钥表（8）内提取一条对应该交易资料的一次性密钥（801）将交易资料解密，以及，收卡银行帐务系统（3）将资料加密或解密后，就会将该条一次性密钥（801）删除或弃置或标记为已用，使该条一次性密钥（801）不会再次被收卡银行帐务系统（3）使用。

17. 如权利要求 1 所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的系统还包括有 ATM 机（9），ATM 机（9）内设有一个唯一的 ATM 机号（901），以及，ATM 机（9）内置有一商户卡（6）。

18. 一种带键盘和显示屏智能卡的支付转账方法，采用如权利要求 1 至 17 中任一项所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的方法包括卡主预先在智能卡（1）的键盘（102）上输入账户密码、支付金额等交易资料，由智能卡（1）从卡内密钥表（7）提取一条未用的一次性密钥（701）将交易资料加密，然后智能卡（1）将已加密交易资料传送到发卡银行帐务系统（4），由发卡银行帐务系统（4）采用与该已加密交易资料对应的一次性密钥（701）将已加密交易资料解密，解密成功后发卡银行帐务系统（4）根据交易资料内容进行相应的支付、转账等银行账户操作。

19. 如权利要求 18 所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下 A 组步骤，是卡主使用智能卡（1）在商店进行支付时的步骤，具体的步骤如下：

A1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入支付金额和账户密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 A 加密成为资料包 B，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 A 的内容包括卡号（106）、支付金额、账户密码等资料；

主芯片（101）将资料包 B、卡号（106）和所述的索引号（702）组成资料包 C；

A2. 商店收款员在 POS 机（2）上输入付款金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，智能卡（1）通过通讯接口（104）将在步骤 A1 中所述的资料包 C 传送给 POS 机（2）；

A3. POS 机（2）通过读卡器读取所述的资料包 C 后，将 POS 机号（201）、付款金额、资料包 C 等资料传送到 POS 机（2）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从卡内密钥表（8）内提取一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 D 加密成为资料包 E，加密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；所述的资料包 D 的内容包括商户卡号（606）、POS 机号（201）、付款金额、资料包 C 等资料；

商户卡（6）内的商户卡芯片（601）将资料包 E、商户卡号（606）、索引号（802）等资料组成资料包 F，然后通过通讯接口（104）将所述的资料包 F 传送给 POS 机（2）；

POS 机（2）通过通讯网络（5）将资料包 F 传送到收卡银行帐务系统（3）；

A4. 收卡银行帐务系统（3）从资料包 F 内容中找到资料包 E、商户卡号（606）、索引号（802），从商户卡号（606）找到对应该商户卡号（606）的商户卡账户，从索引号（802）在该商户卡账户的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 E 解密还原出资料包 D，解密成功后表示该资料包 E 是从该商户卡号（606）所对应的商户卡（6）发出的，解密后收卡银行帐务系统（3）从密钥表（8）中将该一次性密钥（801）删除；

收卡银行帐务系统（3）从资料包 D 中找出资料包 C、商户卡号（606）、POS 机号（201）、付款金额等资料，核对该 POS 机号（201）和该商户卡号（606）是否属于同一商户，核对两者属于同一商户无误后，将资料包 C、商户卡号（606）、付款金额等资料传送到发卡银行帐务系统（4）请求转账支付；

A5. 发卡银行帐务系统（4）收到资料包 C、商户卡号（606）、付款金额等资料后，从资料包 C 内容中找到资料包 B、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 B 解密还原出资料包 A，解密成功后表示该资料包 B 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 A 中找出卡号（106）、支付金额、账户密码等资料，核对支付金额和付款金额相同无误后，发卡银行帐务系统（4）核对账户密码和所述的卡号（106）的智能卡账户结余，核对无误后，从所述的卡号（106）的智能卡账户内转账支付金额的钱到所述的商户卡号（606）在收卡银行帐务系统（3）的商户卡账户；

转账成功后发卡银行帐务系统（4）从所述的智能卡账户的密钥表（7）内提取另一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 1 加密成为资料包 2，加密后发卡银行帐务系统（4）从密钥表（7）中将该另一条一次性密钥（701）删除；所述的资料包 1 的内容包括卡号（106）、商户卡号（606）、已转账支付金额等资料；

发卡银行帐务系统（4）将资料包 2、卡号（106）、该一次性密钥（701）的索引号（702）、商户卡号（606）、已转账支付金额等资料组成资料包 3；

发卡银行帐务系统（4）将资料包 3 传送给收卡银行帐务系统（3）；

A6. 收卡银行帐务系统(3)收到资料包 3 后，从资料包 3 中找到资料包 2、卡号(106)、索引号（702）、商户卡号（606）、已转账支付金额等资料，知道转账成功，将转账支付的交易详细资料储存；

收卡银行帐务系统（3）从所述商户卡号（606）的商户卡账户的密钥表（8）内提取另一条一次性密钥(801)和对应的索引号(802)，以该一次性密钥(801)将资料包 3 加密成为资料包 4，加密后收卡银行帐务系统（3）从密钥表（8）中将该另一条一次性密钥（801）删除；

收卡银行帐务系统（3）将资料包 4、商户卡号（606）、索引号（802）等资料组成资料包 5；

收卡银行帐务系统（3）将资料包 5 通过通讯网络（5）传送给 POS 机（2）；

A7. POS 机（2）收到资料包 5 后，将资料包 5 传送给 POS 机（2）内的商户卡（6）；

商户卡(6)内的商户卡芯片(601)从资料包 5 中找到资料包 4、商户卡号(606)、索引号（802）等资料，从索引号（802）在商户卡芯片（601）的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 4 解密还原出资料包 3，解密成功后表示该资料包 4 是由收卡银行帐务系统（3）所发出的，从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账支付金额等资料，商户卡芯片（601）将该笔交易的资料储存在商户卡芯片（601）内的存储器中，解密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；

商户卡（6）将资料包 3 传送给 POS 机（2）；

POS 机（2）将资料包 3 通过读卡器传送给智能卡（1），并通过 POS 机（2）的显示装置显示已转账支付金额给收款员看，以及打印收条给卡主；

智能卡（1）内的主芯片（101）从资料包 3 中找到资料包 2、卡号（106）、索引号（702）、商户卡号（606）、已转账支付金额等资料，从索引号（702）在主芯片（101）的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 2 解密还原出资料包 1，解密成功后表示该资料包 2 是由发卡银行帐务系统（4）所发出的，主芯片（101）将该笔交易的资料储存在主芯片

（101）内的存储器中，解密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；

主芯片（101）从资料包 1 中找到卡号（106）、商户卡号（606）、已转账支付金额等资料，通过显示装置（103）将已转账支付金额显示给卡主看，以及，主芯片（101）自动将智能卡（1）上锁，上锁后的智能卡（1）要输入正确的开卡口令后才能使用。

20. 如权利要求 18 所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下 B 组步骤，是卡主使用智能卡（1）在 ATM 机（9）进行取款的步骤，具体的步骤如下：

B1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入取款金额和账户密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 A 加密成为资料包 B，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 A 的内容包括卡号（106）、取款金额、账户密码等资料；

主芯片（101）将资料包 B、卡号（106）和所述的索引号（702）组成资料包 C；

B2. 卡主将智能卡（1）放到 ATM 机（9）的读卡器上拍卡，智能卡（1）通过通讯接口（104）将在步骤 A1 中所述的资料包 C 传送给 ATM 机（9）；

B3. ATM 机（9）通过读卡器读取所述的资料包 C 后，将资料包 C 连同 ATM 机号（901）等资料传送到 ATM 机（9）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从卡内密钥表（8）内提取一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 G 加密成为资料包 H，加密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；所述的资料包 G 的内容包括商户卡号（606）、ATM 机号（901）、资料包 C 等资料；

商户卡（6）内的商户卡芯片（601）将资料包 H、商户卡号（606）、索引号（802）组成资料包 J，然后通过通讯接口（104）将所述的资料包 J 传送给 ATM 机（9）；

ATM 机（9）通过通讯网络（5）将资料包 J 传送到收卡银行帐务系统（3）；

B4. 收卡银行帐务系统（3）从资料包 J 内容中找到资料包 H、商户卡号（606）和索引号（802），从商户卡号（606）找到对应该商户卡号（606）的商户卡账户，从索引号（802）在该商户卡账户的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 H 解密还原出资料包 G，解密成功后表示该资料包 H 是从该商户卡号（606）所对应的商户卡（6）发出的，解密后收卡银行帐务系统（3）从密钥表（8）中将该一次性密钥（801）删除；

收卡银行帐务系统（3）从资料包 G 中找出资料包 C、商户卡号（606）、ATM 机号（901）、付款金额等资料，核对该 ATM 机号（901）和该商户卡号（606）是否属于收卡银行的，核对两者属于收卡银行无误后，将资料包 C、商户卡号（606）等资料传送到发卡银行帐务系统（4）请求转账支付；

B5. 发卡银行帐务系统（4）收到资料包 C、商户卡号（606）等资料后，从资料包 C 中找到资料包 B、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 B 解密还原出资料包 A，解密成功后表示该资料包 B 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 A 中找出卡号（106）、取款金额、账户密码等资料，核对取款金额、账户密码和所述的卡号（106）的智能卡账户结余，核对无误后，从所述的卡号（106）的智能卡账户内转账取款金额的钱到所述的商户卡号（606）在收卡银行帐务系统（3）的商户卡账户；

转账成功后发卡银行帐务系统（4）从所述的智能卡账户的密钥表（7）内提取另一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 1 加密成为资料包 2，加密后发卡银行帐务系统（4）从密钥表（7）中将该另一条一次性密钥（701）删除；所述的资料包 1 的内容包括卡号（106）、商户卡号（606）、已转账取款金额等资料；

发卡银行帐务系统（4）将资料包 2、卡号（106）、该一次性密钥（701）的索引号（702）、商户卡号（606）、已转账取款金额等资料组成资料包 3；

发卡银行帐务系统（4）将资料包 3 传送给收卡银行帐务系统（3）；

B6. 收卡银行帐务系统(3)收到资料包3后,从资料包3中找到资料包2、卡号(106)、索引号（702）、商户卡号（606）、已转账取款金额等资料，知道转账成功，将转账支付的交易详细资料储存；

收卡银行帐务系统（3）从所述商户卡号（606）的商户卡账户的密钥表（8）内提取另一条一次性密钥(801)和对应的索引号(802)，以该一次性密钥(801)将资料包3加密成为资料包4，加密后收卡银行帐务系统（3）从密钥表（8）中将该另一条一次性密钥（801）删除；

收卡银行帐务系统（3）将资料包4、商户卡号（606）、索引号（802）等资料组成资料包5；

收卡银行帐务系统（3）将资料包5通过通讯网络（5）传送给ATM机（9）；

B7. ATM机（9）收到资料包5后，将资料包5传送给ATM机(9)内的商户卡（6）；

商户卡(6)内的商户卡芯片(601)从资料包5中找到资料包4、商户卡号(606)、索引号（802）等资料，从索引号（802）在商户卡芯片（601）的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包4解密还原出资料包3，解密成功后表示该资料包4是由收卡银行帐务系统（3）所发出的，从资料包3中找到资料包2、卡号（106）、索引号（702）、商户卡号（606）、已转账取款金额等资料，商户卡芯片（601）将该笔交易的资料储存在商户卡芯片（601）内的存储器中，解密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；

商户卡（6）将资料包3传送给ATM机（9）；

ATM机（9）将资料包3通过读卡器传送给智能卡（1），并通过ATM机（9）的显示装置显示已转账取款金额给卡主看，以及，ATM机（9）吐出取款金额的钞票和打印收条给卡主；

智能卡（1）内的主芯片（101）从资料包3中找到资料包2、卡号（106）、索引号（702）、商户卡号（606）、已转账取款金额等资料，从索引号（702）在主芯片（101）的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包2解密还原出资料包1，解密成功后表示该资料包2是由发卡银行帐务系统（4）所发出的，主芯片（101）将该笔交易的资料储存在主芯片（101）内的存储器中，解密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；

主芯片（101）从资料包 1 中找到卡号（106）、商户卡号（606）、已转账取款金额等资料，通过显示装置（103）将已转账取款金额显示给卡主看，以及，主芯片（101）自动将智能卡（1）上锁，上锁后的智能卡（1）要输入正确的开卡口令后才能使用。

21. 如权利要求 18 所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下 C 组步骤，是卡主使用智能卡（1）在网上进行购物时支付的步骤，具体的步骤如下：

C1. 卡主使用可连线上网的电脑终端（12）连线上网，并进入到购物网站（13），根据购物网站（13）内容的引导，选购所需物品，然后在付款时购物网站（13）显示支付金额和购物网站银行账户号码；

卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入支付金额、账户密码、购物网站银行账户号码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 K 加密成为资料包 L，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 K 的内容包括卡号（106）、购物网站银行账户号码、支付金额、账户密码等资料；

主芯片（101）将资料包 L、卡号（106）和所述的索引号（702）组成资料包 M，并通过显示装置（103）显示给卡主看；

C2. 卡主根据购物网站（13）的网页内容引导，通过电脑终端（12）输入在步骤 C1 中智能卡（1）所显示的资料包 M 的内容；

C3. 电脑终端（12）将卡主所输入的资料包 M 通过互联网络（11）传送到购物网站（13）；

C4. 购物网站（13）将资料包 M、购物网站银行账户号码和付款金额等资料组成资料包 N，然后将资料包 N 传送到收卡银行帐务系统（3）；

C5. 收卡银行帐务系统（3）从资料包 N 中找到资料包 M、购物网站银行账户号码、付款金额等资料，从资料包 M 中找到资料包 L、卡号（106）、索引号（702）等资料；

收卡银行帐务系统（3）核对资料无误后，将资料包 M、购物网站银行账户号码、付款金额等资料传送到所述卡号（106）的发卡银行帐务系统（4）请求转账支付；

C6. 发卡银行帐务系统（4）收到资料包 M、购物网站银行账户号码、付款金额等资料后，从资料包 M 内容中找到资料包 L、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 L 解密还原出资料包 K，解密成功后表示该资料包 L 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 K 中找出卡号（106）、购物网站银行账户号码、支付金额、账户密码等资料，核对支付金额和付款金额相同无误后，发卡银行帐务系统（4）核对账户密码和所述的卡号（106）的智能卡账户结余，核对无误后，从所述的卡号（106）的智能卡账户内转账支付金额的钱到收卡银行帐务系统（3）的购物网站银行账户号码的账户内；

C7. 转账后发卡银行帐务系统（4）通知收卡银行帐务系统（3）转账支付成功；

C8. 收卡银行帐务系统（3）通知购物网站（13）转账支付成功；

C9. 购物网站（13）通过互联网络（11）将转账支付成功信息和支付的详细资料传送到电脑终端（12）给卡主看，并安排将卡主所购买的物品送货给卡主。

22. 如权利要求 18 所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下 D 组步骤，是卡主使用智能卡（1）在网上进行转账的步骤，具体的步骤如下：

D1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入转账金额、账户密码、收款人账户号码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 K 加密成为资料包 L，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述

的资料包 K 的内容包括卡号（106）、收款人账户号码、转账金额、账户密码等资料；

主芯片（101）将资料包 L、卡号（106）和所述的索引号（702）组成资料包 M，并通过显示装置（103）显示给卡主看；

D2. 卡主使用可连线上网的上网终端（12）连线上网，并登入到发卡银行帐务系统（4）的转账网页，根据转账网页内容的引导，通过上网终端（12）输入转账金额、收款人账户号码等资料，以及输入在步骤 D1 中智能卡（1）所显示的资料包 M 的内容；

D3. 上网终端（12）将卡主所输入的资料包 M 通过互联网络（11）传送到发卡银行帐务系统（4）；

D4. 发卡银行帐务系统(4)收到资料包 M 后，从资料包 M 中找到资料包 L、卡号(106)和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 L 解密还原出资料包 K，解密成功后表示该资料包 L 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 K 中找出卡号（106）、收款人账户号码、转账金额、账户密码等资料，核对转账金额、账户密码和所述的卡号（106）的智能卡账户结余及卡主在步骤 D2 中所输入的转账金额、收款人账户号码等资料，核对无误后，从所述的卡号（106）的智能卡账户内转账转账金额的钱到收卡银行帐务系统（3）的收款人账户号码的银行账户内；

D5. 转账后收卡银行帐务系统（3）通知发卡银行帐务系统（4）转账成功；

D6. 发卡银行帐务系统（4）通过互联网络（11）将转账成功信息和转账的详细资料传送到上网终端（12）给卡主看。

23. 如权利要求 18 所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下 E 组步骤，是卡主使用智能卡（1）和手机进行转账的步骤，具体的步骤如下：

E1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主

可以开始使用智能卡（1），并引导卡主输入转账金额、账户密码、收款人账户号码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 K 加密成为资料包 L，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 K 的内容包括卡号（106）、收款人账户号码、转账金额、账户密码等资料；

主芯片（101）将资料包 L、卡号（106）和所述的索引号（702）组成资料包 M，并通过显示装置（103）显示给卡主看；

E2. 卡主将资料包 M 的内容输入到手机中，然后通过手机和移动电话网络（14）以短信或彩信或 USSD 信息将资料包 M 的内容传送到发卡银行帐务系统（4）；

E3. 发卡银行帐务系统(4)收到资料包 M 后，从资料包 M 中找到资料包 L、卡号(106)和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 L 解密还原出资料包 K，解密成功后表示该资料包 L 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 K 中找出卡号（106）、收款人账户号码、转账金额、账户密码等资料，核对转账金额、账户密码和所述的卡号（106）的智能卡账户结余、收款人账户号码等资料，核对无误后，从所述的卡号（106）的智能卡账户内转账转账金额的钱到收卡银行帐务系统（3）的收款人账户号码的银行账户内；

E4. 转账后收卡银行帐务系统（3）通知发卡银行帐务系统（4）转账成功；

E5. 发卡银行帐务系统（4）通过移动电话网络（14）以短信或彩信或 USSD 信息将转账成功信息和转账的详细资料传送到卡主手机给卡主看。

24. 如权利要求 18 所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下 F 组步骤，是卡主使用智能卡（1）和手机进行转账的步骤，具体的步骤如下：

F1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主

可以开始使用智能卡（1），并引导卡主输入转账金额、账户密码、收款人手机电话号码、接收款项密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包 0 加密成为资料包 P，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包 0 的内容包括卡号（106）、收款人手机电话号码、接收款项密码、转账金额、账户密码等资料；

主芯片（101）将资料包 P、卡号（106）和所述的索引号（702）组成资料包 Q，并通过显示装置（103）显示给卡主看；

F2. 卡主将资料包 Q 的内容输入到手机中，然后通过手机和移动电话网络（14）以短信或彩信或 USSD 信息将资料包 Q 传送到发卡银行帐务系统（4）；

F3. 发卡银行帐务系统(4)收到资料包 Q 后，从资料包 Q 中找到资料包 P、卡号(106)和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包 P 解密还原出资料包 0，解密成功后表示该资料包 P 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 0 中找出卡号（106）、收款人手机电话号码、接收款项密码、转账金额、账户密码等资料，核对转账金额、账户密码和所述的卡号（106）的智能卡账户结余等资料，核对无误后，从所述的卡号（106）的智能卡账户内暂时冻结转账金额的钱，等待收款人在指定时间内凭接收款项密码提取该笔款项，例如在 5 分钟内；

发卡银行帐务系统（4）通过移动电话网络（14）发短信或彩信或 USSD 信息给卡主手机，通知卡主已经准备妥该笔转账款项，收款人可在指定时间内凭接收款项密码提取该笔款项；

F4. 收款人在指定时间内用自己的收款人手机通过移动电话网络（14）以短信或彩信或 USSD 信息将接收转账款项信息传送到发卡银行帐务系统（4），所述的接收转账款项信息包括收款人在收卡银行帐务系统（3）的收款人账户号码和接收款项密码；

F5. 发卡银行帐务系统（4）收到接收转账款项信息后，从接收转账款项信息的来源电话号码找到收款人手机电话号码，从收款人手机电话号码在发卡银行帐务

系统（4）中找到在步骤F3中所述的暂时冻结转账转账金额的钱的记录，从接收转账款项信息内容找到收款人账户号码和接收款项密码，核对该信息内的接收款项密码与所述的暂时冻结转账金额的钱的记录中的接收款项密码相同无误后，发卡银行帐务系统（4）将该笔暂时冻结转账金额的钱转账到收卡银行帐务系统（3）内的收款人账户号码的账户；

F6. 转账后收卡银行帐务系统（3）通知发卡银行帐务系统（4）转账成功；

F7. 发卡银行帐务系统（4）通过通过移动电话网络（14）发短信或彩信或USSD信息给收款人手机，通知收款人已经成功接收转账款项及转账金额；

F8. 发卡银行帐务系统（4）通过通过移动电话网络（14）发短信或彩信或USSD信息给卡主手机，通知卡主收款人已经成功接收该笔转账款项和转账金额。

25. 如权利要求18所述的带键盘和显示屏智能卡的支付转账方法，其特征在于，所述的方法包括如下G组步骤，是卡主使用智能卡（1）和手机进行遥距ATM取款的步骤，具体的步骤如下：

G1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1），并引导卡主输入取款金额、账户密码、接收款项密码等资料；

智能卡（1）内的主芯片（101）从卡内密钥表（7）内提取一条一次性密钥（701）和对应的索引号（702），以该一次性密钥（701）将资料包R加密成为资料包S，加密后主芯片（101）从密钥表（7）中将该一次性密钥（701）删除；所述的资料包R的内容包括卡号（106）、接收款项密码、取款金额、账户密码等资料；

主芯片（101）将资料包S、卡号（106）和所述的索引号（702）组成资料包T，并通过显示装置（103）显示给卡主看；

G2. 卡主将资料包T的内容输入到手机中，然后通过手机和移动电话网络（14）以短信或彩信或USSD信息将资料包T的内容传送到发卡银行帐务系统（4）；

G3. 发卡银行帐务系统（4）收到资料包T的内容的信息后，从信息内容中找到资料包S、卡号（106）和索引号（702），从卡号（106）找到对应该卡号（106）的智能卡账户，从索引号（702）在该智能卡账户的密钥表（7）内提取该索引号（702）所对应的一次性密钥（701）将资料包S解密还原出资料包R，解密

成功后表示该资料包 S 是从该卡号（106）所对应的智能卡（1）发出的，解密后发卡银行帐务系统（4）从密钥表（7）中将该一次性密钥（701）删除；

发卡银行帐务系统（4）从资料包 R 中找出卡号（106）、接收款项密码、取款金额、账户密码等资料，核对取款金额、账户密码和所述的卡号（106）的智能卡账户结余等资料，核对无误后，从所述的卡号（106）的智能卡账户内暂时冻结取款金额的钱，等待取款人在指定时间内凭接收款项密码提取该笔款项，例如在 5 分钟内，如果取款人在指定时间过后仍未成功提取该笔款项，发卡银行帐务系统（4）会将该笔款项解冻退回所述的智能卡账户内；

发卡银行帐务系统（4）通过移动电话网络（14）发短信或彩信或 USSD 信息给卡主手机；通知卡主已经准备妥该笔取款款项，取款人可在指定时间内到 ATM 机（9）凭接收款项密码提取该笔款项；

G4. 取款人在指定时间内走到 ATM 机（9）前，在 ATM 机（9）输入卡主的卡号（106）、提款金额、接收款项密码等资料；

G5. ATM 机（9）将卡号（106）、ATM 机号（901）、提款金额、接收款项密码等资料传送到 ATM 机（9）内的商户卡（6）；

商户卡（6）内的商户卡芯片（601）从卡内密钥表（8）内提取一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包 U 加密成为资料包 V，加密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；所述的资料包 U 的内容包括有卡号（106）、提款金额、接收款项密码、商户卡号（606）、ATM 机号（901）等资料；

商户卡（6）内的商户卡芯片（601）将资料包 V、商户卡号（606）、索引号（802）组成资料包 W，然后通过通讯接口（104）将资料包 W 传送给 ATM 机（9）；

ATM 机（9）通过通讯网络（5）将资料包 W 传送到收卡银行帐务系统（3）；

G6. 收卡银行帐务系统（3）从资料包 W 中找到资料包 V、商户卡号（606）和索引号（802），从商户卡号（606）找到对应该商户卡号（606）的商户卡账户，从索引号（802）在该商户卡账户的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包 V 解密还原出资料包 U，解密成功后表示该资料包 V 是从该商户卡号（606）所对应的商户卡（6）发出的，解密后收卡银行帐务系统（3）从密钥表（8）中将该一次性密钥（801）删除；

收卡银行帐务系统（3）从资料包 U 中找出卡号（106）、提款金额、接收款项密码、商户卡号（606）、ATM 机号（901）等资料，核对该 ATM 机号（901）和

该商户卡号（606）是否属于收卡银行的，核对两者属于收卡银行无误后，将卡号（106）、提款金额、接收款项密码、商户卡号（606）等资料传送到发卡银行帐务系统（4）请求转账支付；

G7. 发卡银行帐务系统（4）收到卡号（106）、提款金额、接收款项密码、商户卡号（606）等资料后，从卡号（106）在发卡银行帐务系统（4）中找到在步骤G3中所述的暂时冻结取款金额的钱的记录，核对接收款项密码与所述的暂时冻结取款金额的钱的记录中的接收款项密码是否相同，并核对提款金额与所述的暂时冻结取款金额的钱的记录中的取款金额是否相同，核对两者相同无误后，发卡银行帐务系统（4）将该笔暂时冻结取款金额的钱转账到所述的商户卡号（606）在收卡银行帐务系统（3）的商户卡账户内，并通知收卡银行帐务系统（3）转账成功；

G8. 收卡银行帐务系统（3）收到转账成功通知后，收卡银行帐务系统（3）从所述商户卡号（606）的商户卡账户的密钥表（8）内提取另一条一次性密钥（801）和对应的索引号（802），以该一次性密钥（801）将资料包6加密成为资料包7，加密后收卡银行帐务系统（3）从密钥表（8）中将该另一条一次性密钥（801）删除，所述的资料包6的内容包括卡号（106）、提款金额、商户卡号（606）、ATM机号（901）等资料；

收卡银行帐务系统（3）将资料包7、商户卡号（606）、索引号（802）等组成资料包8；

收卡银行帐务系统（3）将资料包8通过通讯网络（5）传送给ATM机（9）；

G9. ATM机（9）收到资料包8后，将资料包8传送给ATM机（9）内的商户卡（6）；商户卡（6）内的商户卡芯片（601）从资料包8中找到资料包7、商户卡号（606）、索引号（802）等资料，从索引号（802）在商户卡芯片（601）的密钥表（8）内提取该索引号（802）所对应的一次性密钥（801）将资料包7解密还原出资料包6，解密成功后表示该资料包7是由收卡银行帐务系统（3）所发出的，从资料包6中找到卡号（106）、提款金额、商户卡号（606）、ATM机号（901）等资料，商户卡芯片（601）将该笔提款操作的资料储存在商户卡芯片（601）内的存储器中，解密后商户卡芯片（601）从密钥表（8）中将该一次性密钥（801）删除；

商户卡（6）将资料包6传送给ATM机（9）；

ATM 机（9）收到资料包 6 后，通过 ATM 机（9）的显示装置显示提款成功信息及提款金额给取款人看，以及，ATM 机（9）吐出提款金额的钞票和打印收条给取款人；

G10. 发卡银行帐务系统（4）通过移动电话网络（14）发短信或彩信或 USSD 信息给卡主手机，通知卡主取款人已经在指定时间内到 ATM 机（9）提取该笔款项。

26. 一种带键盘和显示屏智能卡的小金额交易支付方法，采用如权利要求 1 至 17 中任一项所述的带键盘和显示屏智能卡的支付系统，其特征在于，所述的方法包括在支付时，通过 POS 机（2）从智能卡（1）内结余记录区所储存的结余金额转移与支付金额相等的部份结余到商户卡（6）内结余记录区所储存的结余金额内，以及，在找续或充值时，通过 POS 机（2）从商户卡（6）内结余记录区所储存的结余金额转移与支付金额相等的部份结余到智能卡（1）内结余记录区所储存的结余金额内。

27. 如权利要求 26 所述的带键盘和显示屏智能卡的小金额交易支付方法，其特征在于，所述的方法包括如下 H 组步骤，是卡主使用智能卡（1）在商店进行小金额支付时的步骤，具体的步骤如下：

H1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1）；

H2. 商店收款员在 POS 机（2）上输入支付金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，POS 机（2）读取智能卡（1）的卡号（106）成功后，POS 机（2）将卡号（106）、POS 机号（201）、支付金额等资料传送到 POS 机（2）内的商户卡（6），商户卡（6）内的商户卡芯片（601）以预定的加密算法 B 将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等支付资料加密后传送回 POS 机（2），由 POS 机（2）将已加密支付资料通过读卡器传送给智能卡（1）；

H3. 智能卡（1）通过通讯接口（104）收到已加密支付资料，以预定的加密算法 B 将已加密支付资料解密还原出卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等资料，核对卡号（106）和支付金额少于小额支付上限金额无误后，智能卡（1）内的主芯片（101）从结余记录区内读取最新的一笔结余记录，并核对所述的结余记录内的结余金额不少于支付金额，核对无误后将结余金额减

去支付金额计算出新的结余金额，然后将新的结余金额写进结余记录区内和将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等资料写进小额支出区内，并以预定的加密算法 A 将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等小额交易资料加密，通过通讯接口（104）传送给 POS 机（2），并通过显示装置（103）显示支付金额和最新结余给卡主看，以及，主芯片（101）自动将智能卡（1）上锁，上锁后的智能卡（1）要输入正确的开卡口令后才能使用；

H4. POS 机（2）通过读卡器读取所述的已加密小额交易资料后，将已加密小额交易资料传送到 POS 机（2）内的商户卡（6），商户卡（6）内的主芯片（101）以预定的加密算法 A 将已加密小额交易资料解密，解密成功后还原出卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等小额交易资料，核对资料无误后将卡号（106）、商户卡号（606）、POS 机号（201）、支付金额等资料写进收款记录区内，并从结余记录区内读取最新的一笔结余记录，将所述的结余记录内的结余金额加上支付金额计算出新的结余金额，然后将新的结余金额写进结余记录区内，以及，商户卡（6）向 POS 机（2）发出支付成功信息；

H5. POS 机（2）收到支付成功信息后，立即打印收条给卡主，小额支付操作完成。

28. 如权利要求 26 所述的带键盘和显示屏智能卡的小金额交易支付方法，其特征在于，所述的方法包括如下 J 组步骤，是卡主使用现钞付款，商户将找续零钱存入卡主的智能卡（1）的步骤，具体的步骤如下：

J1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1）；

J2. 卡主以现钞付款后，商店收款员在 POS 机（2）上输入支付金额和现钞金额后，POS 机（2）计算出找续金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，POS 机（2）读取智能卡（1）的卡号（106）成功后，POS 机（2）将卡号（106）和找续金额传送给 POS 机（2）内的商户卡（6），商户卡（6）核对找续金额少于小额支付上限金额后，商户卡（6）内的商户卡芯片（601）从结余记录区内读取最新的一笔结余记录，并核对所述的结余记录内的结余金额不少于找续金额，核对无误后将结余金额减去找续金额计算出新的结余金额，然后将新的结余金额写进结余记录区内和将卡号（106）、商户卡号（606）、

POS 机号（201）、找续金额等资料写进支出记录区内，并以预定的加密算法 B 将卡号（106）、商户卡号（606）、POS 机号（201）、找续金额等小额找续资料加密，通过通讯接口（604）传送给 POS 机（2）；

J3. POS 机（2）通过读卡器所述的已加密小额找续资料传送给智能卡（1），智能卡（1）内的主芯片（101）以预定的加密算法 B 将已加密小额找续资料解密，解密成功后还原出卡号（106）、商户卡号（606）、POS 机号（201）、找续金额等小额找续资料，核对资料无误后将卡号（106）、商户卡号（606）、POS 机号（201）、找续金额写进小额存入区内，并从结余记录区内读取最新的一笔结余记录，将所述的结余记录内的结余金额加上找续金额计算出新的结余金额，然后将新的结余金额写进结余记录区内，以及，通过显示装置（103）显示找续金额和最新结余，并向 POS 机（2）发出找续成功信息；

J4. POS 机（2）收到找续成功信息后，立即打印收条给卡主，小额找续操作完成。

29. 如权利要求 26 所述的带键盘和显示屏智能卡的小金额交易支付方法，其特征在于，所述的方法包括如下 K 组步骤，是卡主在商户使用现钞付款充值智能卡（1）的步骤，具体的步骤如下：

K1. 卡主在智能卡（1）上的键盘（102）输入开卡口令，智能卡（1）内的主芯片（101）核对开卡口令无误后，通过显示装置（103）显示提示信息，提示卡主可以开始使用智能卡（1）；

K2. 卡主将充值金额的现钞交给商户的收款员，商店收款员点收现钞后在 POS 机（2）上输入充值金额，然后卡主将智能卡（1）放到 POS 机（2）的读卡器上拍卡，POS 机（2）读取智能卡（1）的卡号（106）成功后，POS 机（2）将卡号（106）和充值金额传送给 POS 机（2）内的商户卡（6），商户卡（6）核对充值金额少于小额支付上限金额后，商户卡（6）内的商户卡芯片（601）从结余记录区内读取最新的一笔结余记录，并核对所述的结余记录内的结余金额不少于充值金额，核对无误后将结余金额减去充值金额计算出新的结余金额，然后将新的结余金额写进结余记录区内和将卡号（106）、商户卡号（606）、POS 机号（201）、充值金额等资料写进支出记录区内，并以预定的加密算法 B 将卡号（106）、商户卡号（606）、POS 机号（201）、充值金额等充值资料加密，通过通讯接口（604）传送给 POS 机（2）；

K3. POS 机（2）通过读卡器所述的已加密充值资料传送给智能卡（1），智能卡（1）内的主芯片（101）以预定的加密算法 B 将已加密充值资料解密，解密成功后还原出卡号（106）、商户卡号（606）、POS 机号（201）、充值金额等充值资料，核对资料无误后将卡号（106）、商户卡号（606）、POS 机号（201）、充值金额写进充值记录区内，并从结余记录区内读取最新的一笔结余记录，将所述的结余记录内的结余金额加上充值金额计算出新的结余金额，然后将新的结余金额写进结余记录区内，以及，通过显示装置（103）显示充值金额和最新结余，并向 POS 机（2）发出充值成功信息；

K4. POS 机（2）收到充值成功信息后，立即打印收条给卡主，充值操作完成。

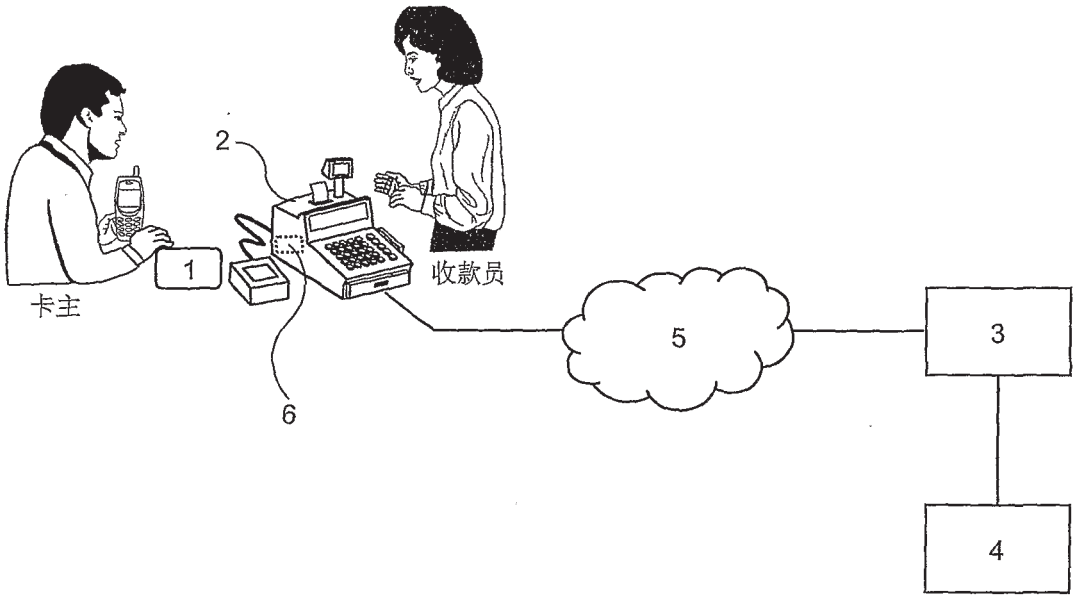

图 1

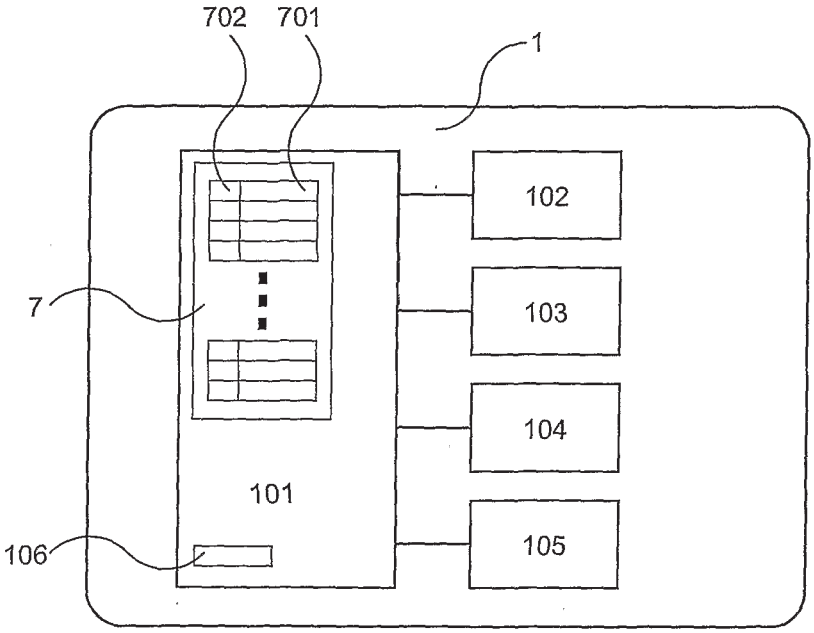

图 2

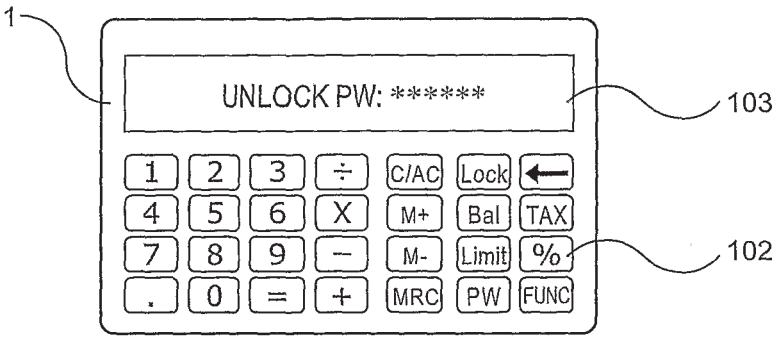
1
UNLOCK PW: ******
103
1 2 3 ÷ C/AC Lock
4 5 6 X M+ Bal TAX
7 8 9 − M- Limit %
. 0 = + MRC PW FUNC
102

图 3

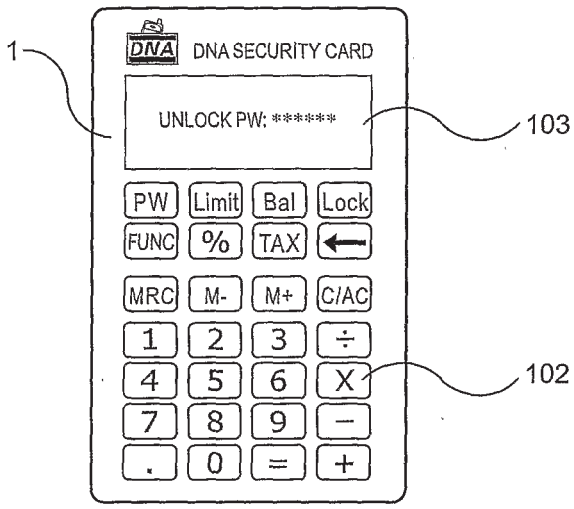
1
DNA SECURITY CARD
UNLOCK PW: ******
103
PW Limit Bal Lock
FUNC % TAX
MRC M- M+ C/AC
1 2 3 ÷
4 5 6 X
7 8 9 −
. 0 = +
102

图 4

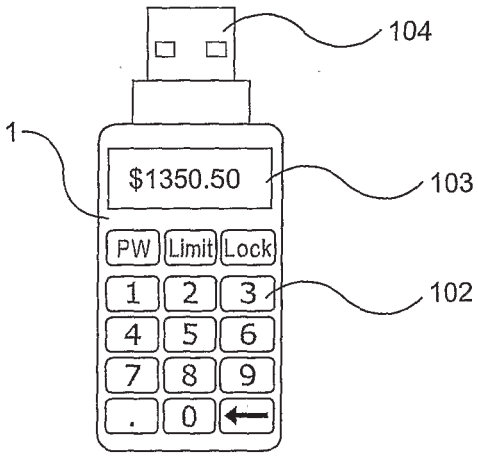
104
1
$1350.50
103
PW Limit Lock
1 2 3
4 5 6
7 8 9
. 0
102

图 5

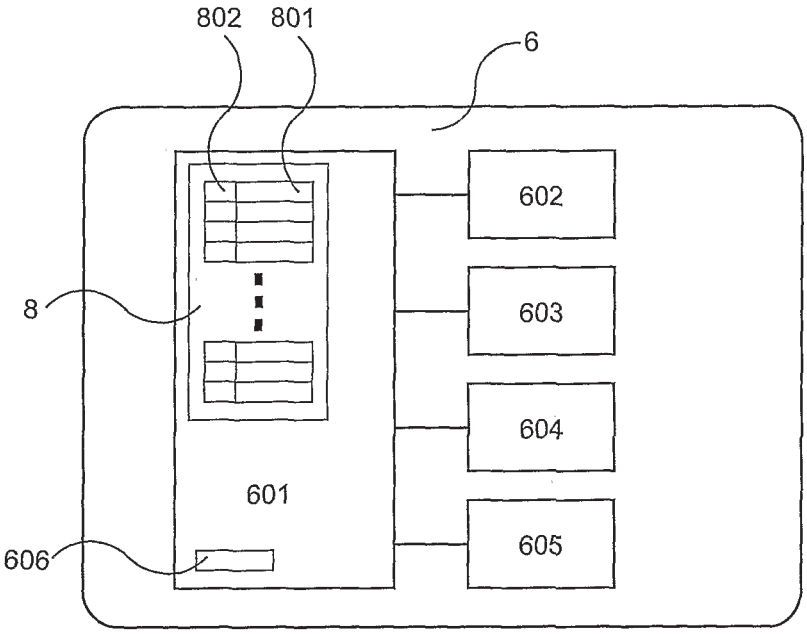

图 6

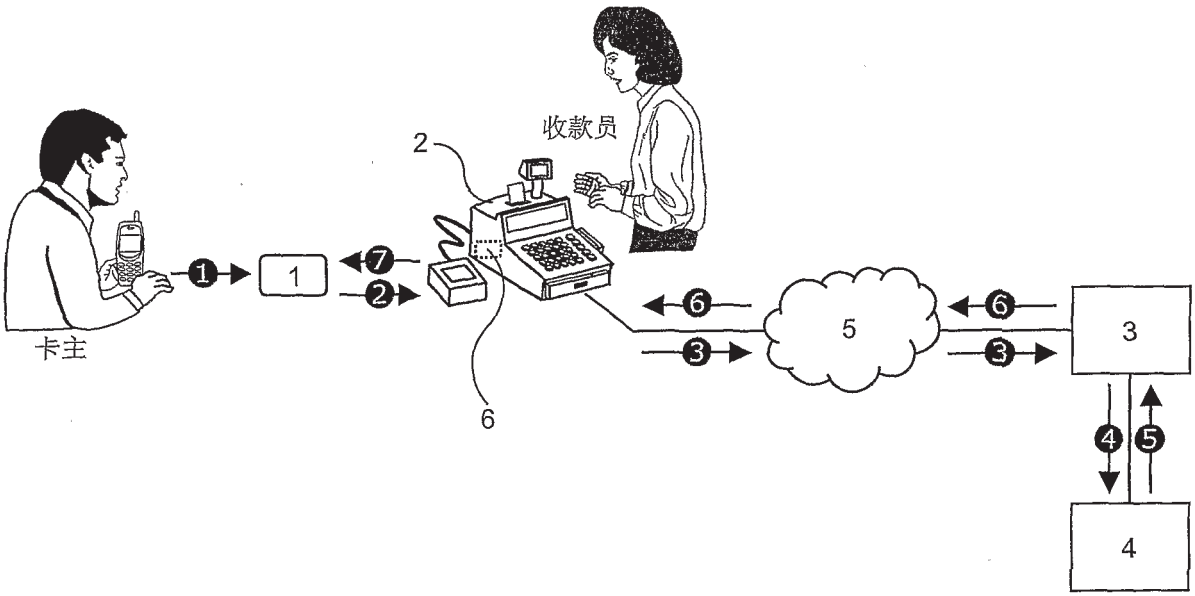

图 7

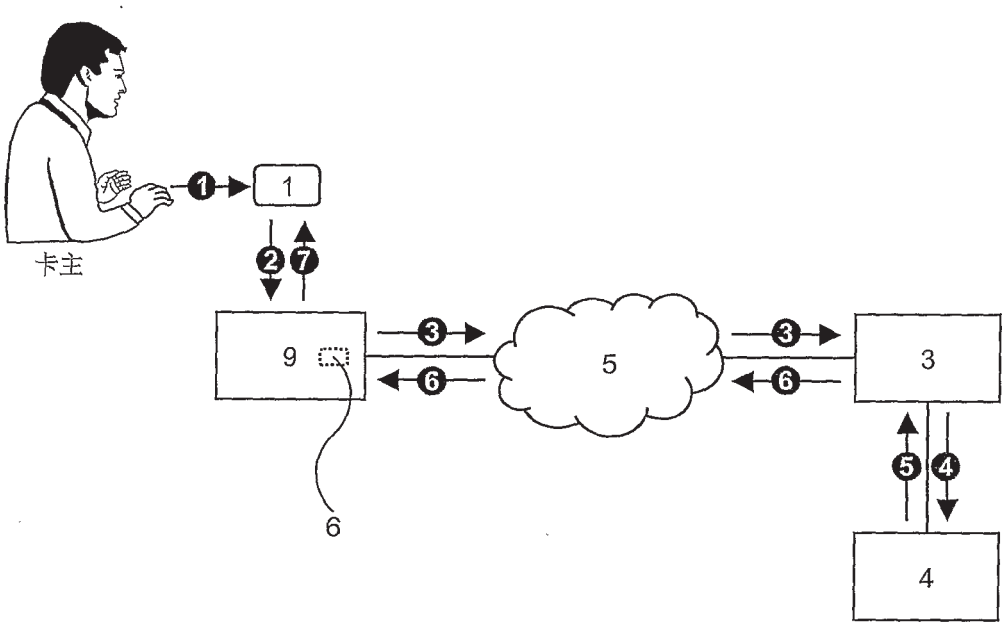

图 8

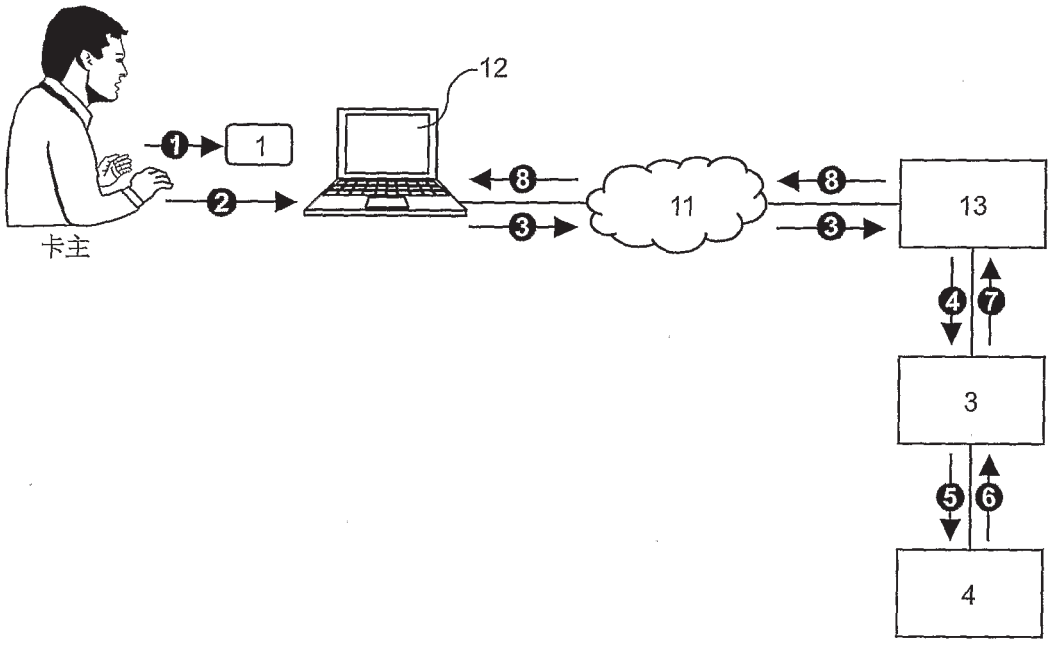

图 9

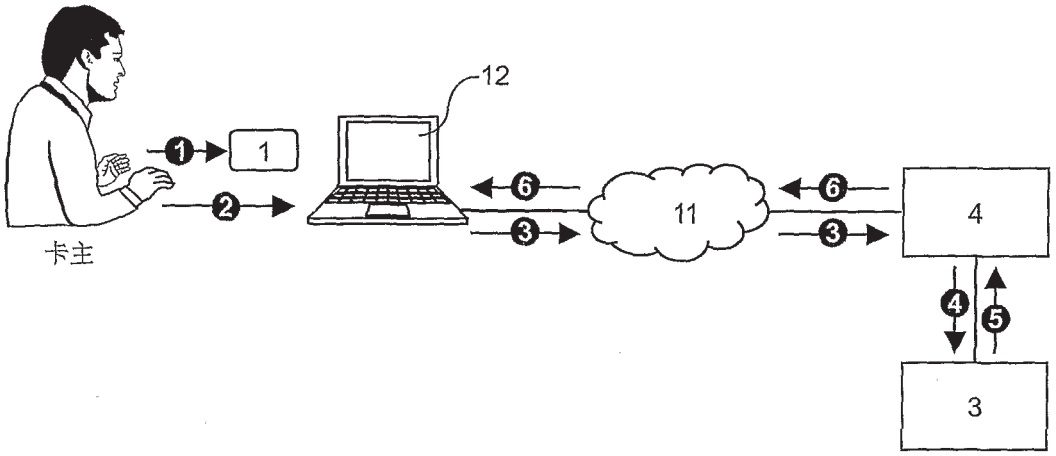

图 10

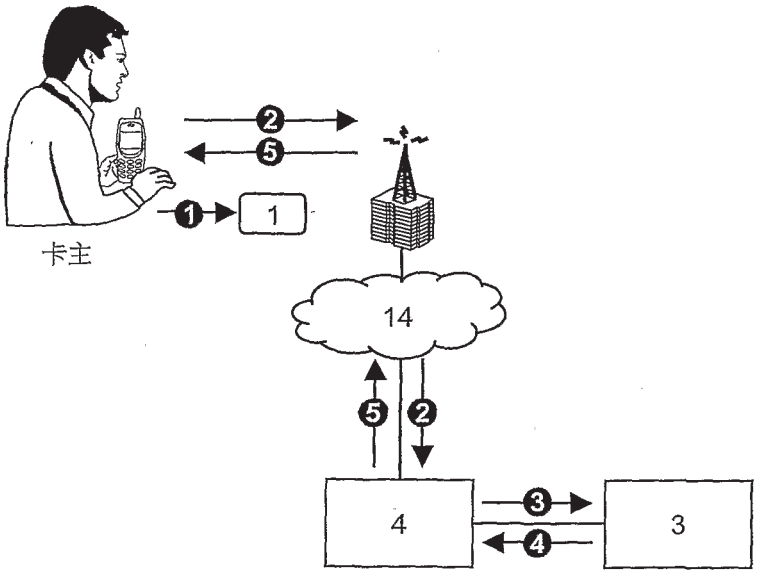

图 11

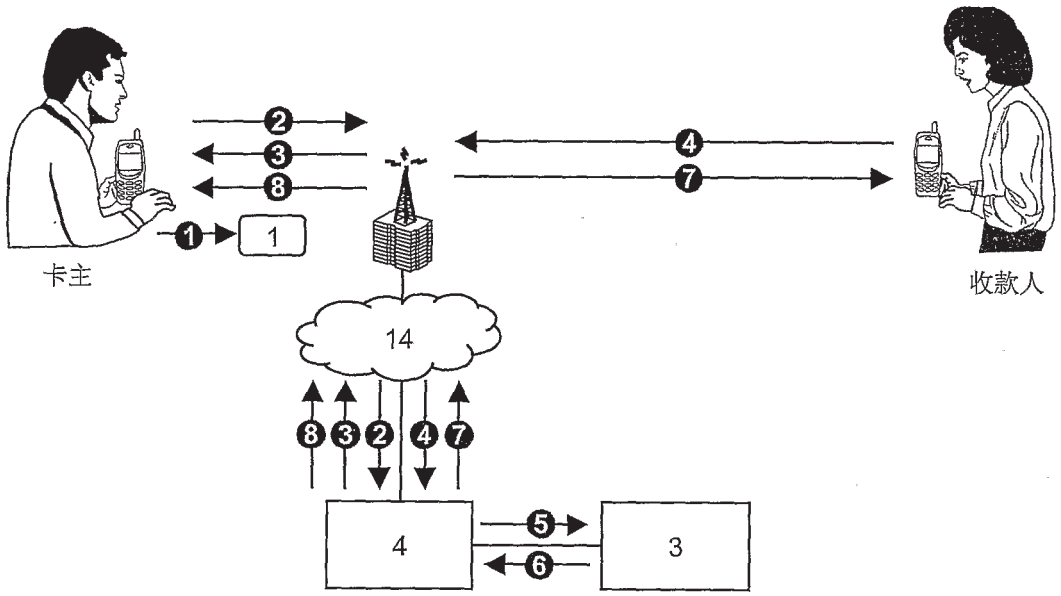

图 12

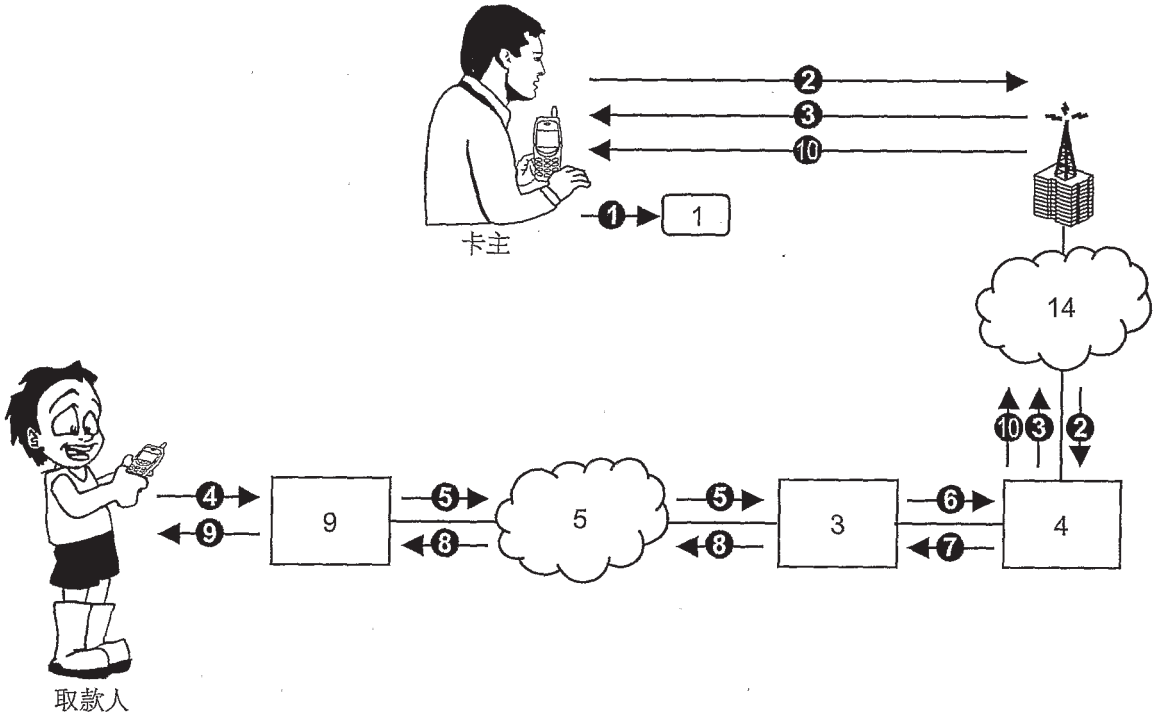

图 13

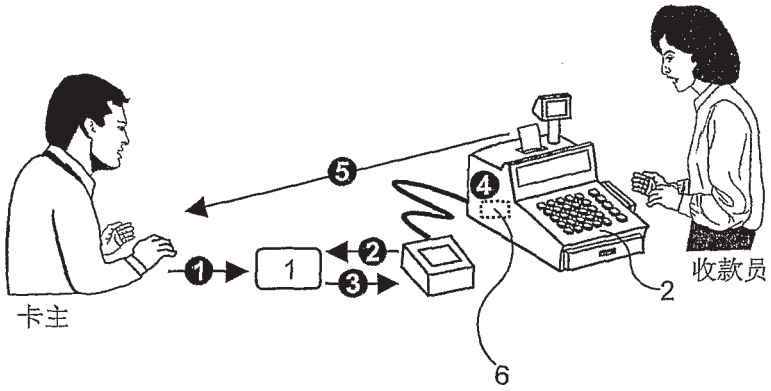

图 14

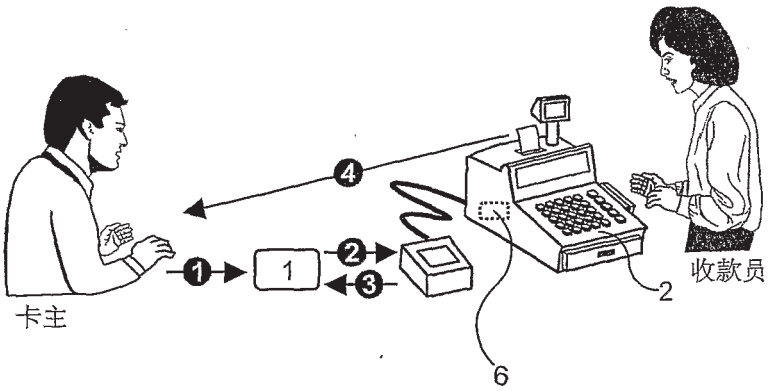

图 15

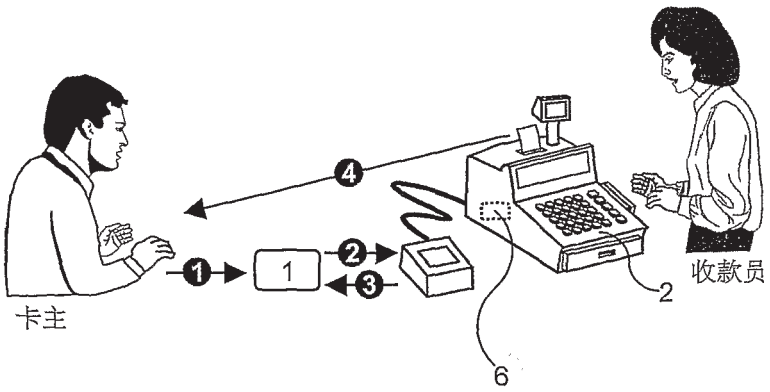

图 16