(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 2009/018684 A1

(51) 国际专利分类号:
H04M 1/68 (2006.01) *H04L 9/32* (2006.01)
H04L 9/16 (2006.01)

(21) 国际申请号: PCT/CN2007/002383

(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,

［见续页］

(54) **Title:** THE KEYBOARD FOR ENCRYPTING AND AUTHENTICATING AGAINST TROJAN HORSE WITH ONE TIME KEY

(54) **发明名称:** 可对抗木马程式采用用完即弃一次性密钥的加密认证键盘

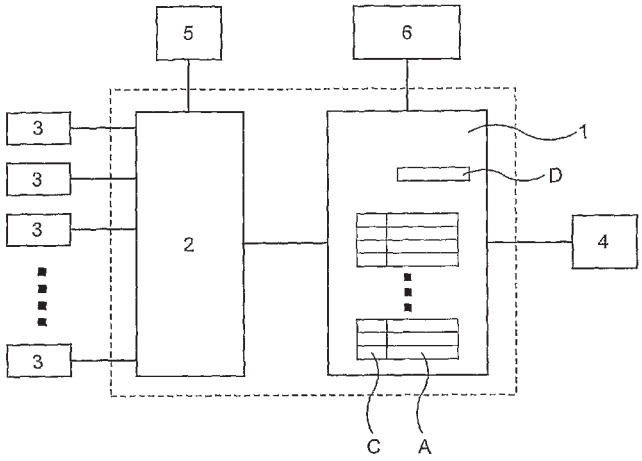

图1 / Fig. 1

(57) **Abstract:** The keyboard for encrypting and authenticating has normal mode and encryption mode. In the normal mode, the information inputted in the keyboard (3) is outputted through the communication interface (4) directly. In the encryption mode, the information inputted in the keyboard (3) is saved on the main chip (1) temporarily. When all the information is inputted, and the mode key (5) is pressed to change the encryption mode to the normal mode, the main chip (1) uses one key (A) which is not used before to encrypt the saved information, and outputs it through the communication interface (4). Because the information is not outputted in the encryption mode, and the information is encrypted by the one-time key before it is outputted. So even the encrypted information is obtained by the Trojan horse of hacker, the information can not be decrypted correctly.

［见续页］

WO 2009/018684 A1

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。

(57) 摘要：

一种加密认证键盘，具有标准模式和加密模式，在标准模式下，在按键（3）上输入的资料会直接在通讯接口（4）输出，在加密模式下，在按键（3）上输入的资料会暂时保存在主芯片（1），输入完成后，按一次模式键（5）切换为标准模式时，主芯片（1）就会按预定程序提取一条未用的密钥（A）将暂存的资料加密，然后通过通讯接口（4）输出。本发明的优点是于加密模式下在键盘输入的重要资料不会即时输出，在输入完成后由键盘通过一次性密钥将资料加密后送出，即使黑客采用木马程式截取了从键盘送出的已加密资料，也无法破解出用户所输入的重要资料，特别适合用于网上银行服务，通过本发明的键盘可以保密输入账户号码、口令、金额等敏感重要资料。

可对抗木马程式采用用完即弃一次性密钥的加密认证键盘

【技术领域】

本发明涉及信息传送安全领域，特别是涉及一种用于认证的加密认证键盘。

【技术背景】

由于现时一般网络的安全性问题，经常会发生黑客盗用他人账户的事件，一些对网络安全性要求高的机构，例如金融机构，采用一些双因素认证手段来对抗黑客，例如采用保安编码器（Token Device），用户登入金融机构的服务器时，由保安编码器产生一个编码，用户除了要输入正确的用户口令外，还要输入正确的编码才能登入金融机构的服务器。这些保安编码器一般内置有一条密钥，使用时由保安编码器根据时间等因素，通过复杂的算法计算产生一个保安编码，而在金融机构的服务器内也采用相同的一条密钥，根据时间等因素通过相同的算法计算产生一个编码，如果金融机构的服务器所产生的编码与接收到由保安编码器所产生的保安编码相同，就可认证该保安编码器的身份，加上核对用户口令，要同时通过保安编码和用户口令的认证，才能成功登入。这种双因素认证手段虽然可以改善网络安全的问题，但仍然有部份网络保安问题未妥善解决，例如一些黑客采用各种入侵方法，将木马程式置于用户的计算机内，在用户连线到金融机构的服务器时，通过木马程式截取用户在计算机键盘上按键输入的资料，包括账户号码、账户口令和用户输入的保安编码等，然后黑客根据截取到资料，即时登入金融机构的服务器，盗取用户账户内的钱。很多人由

于害怕自己的计算机可能会被黑客入侵安装了木马程式，所以不敢使用金融机构的网上交易服务，这是一个极待解决的问题。

【发明内容】

本发明的目的，在于提供一种具有加密认证功能的键盘，能将用户从键盘上输入的重要敏感的资料加密后输出，避免这些重要敏感的资料在传送过程中外泄。

本发明的目的是这样实现的，采用这样一种加密认证键盘，用于认证身份和加密资料，其特征在于，所述的键盘主要结构包括有主芯片（1）、键盘控制器（2）、按键（3）、通讯接口（4）、模式键（5）、显示装置（6），所述加密认证键盘，具有标准模式和加密模式，在标准模式下，在按键（3）上输入的资料会直接在通讯接口（4）输出，在加密模式下，在按键（3）上输入的资料会暂时保存在主芯片（1），输入完成后，按一次模式键（5）切换为标准模式时，主芯片（1）就会按预定程序提取一条未用的密钥（A）将暂存的资料加密，然后通过通讯接口（4）输出。

其中，

主芯片（1）内设有 CPU 和存储器，并与键盘控制器（2）、通讯接口（4）、显示装置（6）等部件相连接，按预定程序运作，实现认证用户在服务器的身份和各项预定功能，包括将用户在加密模式下输入的资料加密、通过显示装置（6）显示提示信息、通过通讯接口（4）发送资料等，以及，键盘控制器（2）与各按键（3）及模式键（5）相连接，按预定程序运作，实现读取用户通过各按键（3）输入的资料，将用户输入的资料传送到主芯片（1）作进一步处理；

以及，

主芯片（1）将用户在加密模式下通过各按键（3）输入的资料，以密钥（A）将输入的资料加密，再通过通讯接口（4）传送给服务器，由服务器使用与该密钥（A）相配对的密钥（B）将资料解密还原出用户所输入的资料，并核对资料内容，核对无误后表示用户的身份认证成功，然后服务器才会根据资料内容进行相应的操作。

以及，

本发明的加密认证键盘的主芯片（1）在加密模式下，用户在各按键（3）上输入的资料会即时由键盘控制器（2）传送到主芯片（1），由主芯片（1）通过显示装置（6）即时将用户所输入的资料显示出来，并将所述的资料暂时保存在主芯片（1）内。

当主芯片（1）内暂存的资料到达指定的大小时，或主芯片（1）的工作模式由加密模式切换为标准模式时，主芯片（1）会按预定程序从主芯片（1）内提取一条未用的密钥（A）和对应该密钥（A）的索引号（C），使用该密钥（A）将在加密模式下暂存的资料连同芯片编号（D）进行加密成为密文，然后将密文、索引号（C）、芯片编号（D）等组成认证资料包，并将该认证资料包通过通讯接口（4）输出传送给服务器，由服务器采用与该密钥（A）相配对的密钥（B）将密文解密还原出用户所输入的资料，以及，主芯片（1）将暂存的资料加密后，就会将暂存的资料删除，并将该条密钥（A）删除或弃置或标记为已用，使该条密钥（A）不会再次被主芯片（1）使用。

这样就实现了本发明的目的。

本发明的优点是用户可于加密模式下在键盘输入的重要资料，而且是采用一次性密钥将重要资料加密后才由键盘送出，即使黑客采用木马程式截

取了从键盘送出的已加密资料，也无法破解出用户所输入的重要资料的内容，本发明的键盘特别适合应用于要求高度安全性的网上银行服务，通过本发明的键盘可以保密输入账户号码、账户口令、金额等敏感重要资料。

【附图说明】

图 1 是本发明的加密认证键盘的第一实施例的方框结构说明图；

图 2 是本发明的加密认证键盘的第二实施例的方框结构说明图；

图 3 是本发明的加密认证键盘的第三实施例的形像化立体示意图；

图 4 是本发明的加密认证键盘的第四实施例的形像化立体示意图；

图 5 是本发明的加密认证键盘的第五实施例的形像化立体示意图；

图 6 是本发明的加密认证键盘的第六实施例的形像化立体示意图；

图 7 是本发明的加密认证键盘的第七实施例的方框结构说明图；

图 8 是本发明的加密认证键盘的第八实施例的形像化立体示意图；

图 9 是本发明的加密认证键盘的第九实施例的形像化立体示意图。

图中，相同的数字代表相同的装置、部件器件，附图是示意性的，用以说明本发明的键盘的主要特征和构成。

【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。

参阅图 1，图 1 是本发明的加密认证键盘的第一实施例的方框结构说明图，图中示出的加密认证键盘主要结构包括有主芯片（1）、键盘控制器（2）、按键（3）、通讯接口（4）、模式键（5）、显示装置（6），其中，主芯片（1）内设有 CPU 和存储器，并与键盘控制器（2）、通讯接口（4）、显

示装置（6）等部件相连接，按预定程序运作，实现认证用户在服务器的身份和各项预定功能，包括将用户在加密模式下输入的资料加密、通过显示装置（6）显示提示信息、通过通讯接口（4）发送资料等，以及，键盘控制器（2）与各按键（3）及模式键（5）相连接，按预定程序运作，实现读取用户通过各按键（3）输入的资料，将用户输入的资料传送到主芯片（1）作进一步处理；以及，主芯片（1）将在加密模式下用户通过各按键（3）输入的资料，以密钥（A）将输入的资料加密，再通过通讯接口（4）传送给服务器，由服务器使用与该密钥（A）相配对的密钥（B）将资料解密还原出用户所输入的资料，并核对资料内容，核对无误后表示用户的身份认证成功，然后服务器才会根据资料内容进行相应的操作。

其中，

所述的通讯接口（4）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、或USB接口、或RS-232接口、或PS2键盘接口。

继续参阅图 1，图中示出的主芯片（1）内还包括有一个唯一的芯片编号（D），并设有多条密钥（A）和多个索引号（C），每一个索引号（C）对应一条密钥（A），以及，各个索引号（C）是互不相同的。

此外，本发明的加密认证键盘的主芯片（1）的工作模式包括有标准模式和加密模式，其中，在标准模式下，用户在按键（3）上输入的资料会即时由键盘控制器（2）传送到主芯片（1），由主芯片（1）将用户输入的资料直接转到通讯接口（4）输出；在加密模式下，用户在按键（3）上输入的资料会即时由键盘控制器（2）传送到主芯片（1），由主芯片（1）通过显示装置（6）即时将用户所输入的资料显示出来，并将所述的资料暂时保存在主芯片（1）内；当主芯片（1）的工作模式由加密模式切换为标准模

式时，或主芯片（1）内暂存的资料到达指定的大小时，例如暂存的资料的大小为16位元组时，主芯片（1）会按预定程序从主芯片（1）内提取一条未用的密钥（A）和对应该密钥（A）的索引号（C），使用该密钥（A）将在加密模式下暂存的资料连同芯片编号（D）进行加密成为密文，然后将密文、索引号、芯片编号（D）等组成认证资料包，并将该认证资料包通过通讯接口（4）输出给服务器，以及，主芯片（1）将暂存的资料加密后，就会将该条密钥（A）删除或弃置或标记为已用，使该条密钥（A）不会再次被主芯片（1）使用。

在服务器方面，服务器内设有多个认证账户，每一个认证账户对应一个键盘的主芯片（1），认证账户内储存有该账户所对应的主芯片（1）的芯片编号（D）和一个账户密码，每一认证账户内储存有多条密钥（B）和多个索引号（C），每一个索引号（C）对应一条密钥（B），

以及，

每一认证账户内的密钥（B）与该账户对应的主芯片（1）内的密钥（A）成配对关系，每一条密钥（B）有一条相配对的密钥（A），每一对相配对的密钥（A）和密钥（B）它们所对应的索引号（C）是相同的。

在设置方面，使用本发明的加密认证键盘前，要预先在服务器开设一个认证账户，并由服务器通过各种方法随机方式产生多对密钥和多个顺序的索引号（C），每一对密钥分配一个索引号（C），然后将每一对密钥分别连同所分配的索引号（C）储存到加密认证键盘的主芯片（1）和认证账户内，储存到主芯片（1）的称为密钥（A），而储存到认证账户的称为密钥（B），如果采用的加密算法是非对称密码算法，密钥（A）和密钥（B）就是一对互相配对的密钥，如果采用的加密算法是对称密码算法，密钥（A）

和密钥（B）就是一对相同的密钥，当使其中一条密钥（A）将资料加密后，可以使用与该密钥（A）相配对的密钥（B）将资料解密。在加密和解密算法方面，可以采用各类不同的算法，例如数据加密标准（Data Encryption Standard - DES）、三重数据加密标准（Triple - DES）、RSA 加密演算法（RSA algorithm）、一次性密码（One Time Pad）、公钥基础架构（Public Key Infrastructure - PKI）等算法，都可很好地实现本发明的目的。

继续参阅图 1，图中示出的模式键（5）主要用于选择主芯片（1）的工作模式，在标准模式下，当用户按一次模式键（5）后，主芯片（1）立即将工作模式切换为加密模式，以及，当用户按一次模式键（5）后，主芯片（1）立即将工作模式切换为标准模式。

本发明的键盘的主芯片（1）还设有开锁口令，在主芯片（1）的工作模式由标准模式切换为加密模式前，用户必须通过按键（3）输入正确的开锁口令，主芯片（1）才将工作模式切换为加密模式。这样可进一步加强本发明的加密认证键盘的安全性。

本发明的加密认证键盘可以应用于一些需要将重要资料传给与服务器的终端机，例如计算机、手机、机顶盒遥控器等终端机，在用户使用设置了本发明的加密认证键盘的终端机与服务器连线时，当输入一些重要资料时，例如账户号码、口令、支付金额、服务确认信息等，可将键盘切换至加密模式，然后才在键盘上输入重要资料，输入完成后用户只要按一次模式键（5），主芯片（1）就会将用户所输入的资料加密成为认证资料包传送给服务器，服务器每次接收到由键盘的主芯片（1）通过通讯接口（4）输出的认证资料包时，从认证资料包内容找出密文、索引号（C）、芯片编号（D），从芯片编号（D）在服务器内找到该芯片编号（D）对应的认证账

户，从认证账户内提取一条与该索引号（C）对应对的密钥（B）将密文解密还原出用户所输入的资料及芯片编号（D），解密成功后核对芯片编号（D）无误后，服务器就可确认该认证资料包是从拥有该芯片编号（D）的主芯片（1）所发出的，以及，服务器将资料解密后，就会将该条密钥（B）删除或弃置或标记为已用，使该条密钥（B）不会再次被服务器使用。

在本说明书中，服务器是指用户要访问的计算机主机，例如各类网上银行的服务器，资料库服务器、电邮服务器等等各类需要认证用户身份的计算机主机或计算机系统或计算机程序等。此外，加密认证键盘将已加密的资料输出给服务器时，已加密的资料是通过包括与加密认证键盘相连接的终端机、网络等设备传送到服务器，为了方便说明，在本说明书中将有关的描述省略，只简单地概括为将资料输出给服务器。

参阅图 2，图 2 是本发明的加密认证键盘的第二实施例的方框结构说明图，图中示出的主芯片（1）主要结构包括有密钥卡（101）、接口电路（102）、连接器（103），其中，密钥卡（101）是单独的，与其它部件相隔开的部件，和接口电路（102）是通过连接器（103）相连接，接口电路（102）与键盘控制器（2）、通讯接口（4）、模式键（5）、显示装置（6）等部件相连接，密钥卡（101）内设有 CPU 和存储器、芯片编号（D）、多条密钥（A）和多个索引号（C），以及，所述的连接器（103）可以是 USB 接口连接器、或 SD 记忆卡接口连接器、或 MINI-SD 记忆卡接口连接器、或 MMC 记忆卡接口连接器、或 RS-MMC 记忆卡接口连接器等记忆卡或忆卡装置的接口连接器。

第二实施例与第一实施例相比，不同之处在于第二实施例中，将主芯片（1）一分为二分为密钥卡（101）和接口电路（102）两部份，其中接口电

路（102）部份与键盘控制器（2）、按键（3）、通讯接口（4）、模式键（5）、显示装置（6）等部件设置于键盘内，并且通过连接器（103）供密钥卡（101）插接，当密钥卡（101）通过连接器（103）插接到键盘后，用户就可在加密模式下通过密钥卡（101）将输入的资料加密。这样键盘与密钥卡（101）分离的设计，可以方便不同的人使用同一个的加密认证键盘，只要用户将自己的密钥卡（101）插到键盘内，该键盘就立即变成为用户个人的加密认证键盘，用完后将密钥卡（101）拔离键盘，该键盘就可供其他人使用。

参阅图 3 至图 5，图 3 是本发明的加密认证键盘的第三实施例的形像化立体示意图，图 4 是本发明的加密认证键盘的第四实施例的形像化立体示意图，图 5 是本发明的加密认证键盘的第五实施例的形像化立体示意图，图 3 至图 5 分别示出了本发明应用于不出终端设备的例子，包括图 3 所示的计算机键盘、图 4 所示的手机键盘、图 5 所示的机顶盒遥控器键盘等。以上各例子用以说明本发明的特点，本发明的加密认证键盘可以应用于所有设有键盘供用户输入资料的装置，在不离开本发明的精神情况下，实施细节可以作一些调整，例如将图 1 中所示的虚线部份的主芯片（1）与键盘控制器（2）合并为一个控制器，又例如将图 2 中所示的虚线部份的接口电路（102）、连接器（103）与键盘控制器（2）等合并为一个控制器，或将主芯片（1）、键盘控制器（2）、通讯接口（4）等合并为一个整体，也可很好都实现本发明的目的，都是属于本发明的保护范围。

参阅图 6，图 6 是本发明的加密认证键盘的第六实施例的形像化立体示意图，图中示出的是一个便携式的小型无线键盘，第六实施例的主要结构与第二实施例基本相同，不同之处在于第六实施例的加密认证键盘的通讯

接口（4）是采用无线通讯方式的接口，可以是红外线装置、或蓝芽装置、或配合智能卡无线阅读器使用的无线通讯装置，或其他的无线通讯装置。本实施例的加密认证键盘可以用于各类信用卡、借记卡等银行卡的身份认证用途，图 6 中示出的密钥卡（101）就是由金融机构发出的银行卡，包括各类信用卡、借记卡等银行卡，在支付时配合加密认证键盘和商店的 POS 机使用。支付时要将密钥卡（101）放入加密认证键盘的连接器（103）内，输入银行账户密码和金额，由加密认证键盘将用户输入的资料加密，然后将卡放到 POS 机上读卡，将已加密资料通过 POS 机传送到银行的账务服务器，由银行的账务服务器将已加密的资料解密和核对资料内容来验证持卡人的身份，验证成功后银行才进行相关的支付操作。

参阅图 7，图 7 是本发明的加密认证键盘的第七实施例的方框结构说明图，图中示出的的加密认证键盘的结构还包括有储存装置接口（7），所述的储存装置接口（7）与外接的储存装置（8）相连接，主要用于将认证资料包通过储存装置接口（7）储存到外接的储存装置（8），以及，所述的储存装置（8）包括各类 USB 记忆装置、SD 记忆卡、Mini-SD 记忆卡、MMC 记忆卡、RS-MMC 记忆卡等记忆装置。本实施例的加密认证键盘除了可将加密后的资料即认证资料包通过通讯接口（4）即时输出外，更可将认证资料包储存在储存装置（8）内，然后通过其他途径传送到服务器。

参阅图 8，图 8 是本发明的加密认证键盘的第八实施例的形像化立体示意图，本实施例与前面各实施例相比，不同之处在于第八实施例的加密认证键盘的显示装置（6）是外接的，是与加密认证键盘前独分离的，显示装置（6）既是计算机（9）的显示器，也是加密认证键盘的显示装置（6），如图 8 所示，显示装置（6）通过电缆（601）与加密认证键盘相连接，同

时显示装置（6）通过另一电缆（602）与计算机（9）的显示器接口相连接，此外，加密认证键盘的通讯接口（4）过键盘电缆（401）与计算机（9）的键盘接口相连接，在加密认证键盘的标准模式下，在按键（3）上输入的资料会直接在通讯接口（4）输出到计算机（9）；在加密模式下，在按键（3）上输入的资料会即时由键盘控制器（2）传送到主芯片（1），由主芯片（1）将输入的资料即时传送给显示装置（6），并且主芯片（1）会将输入述的资料暂时保存在主芯片（1）内，当显示装置（6）收到加密认证键盘传送来的资料，显示装置（6）会立即按预定的程序，将收到的资料在显示装置（6）的屏幕上显示出来，当加密认证键盘切换回标准模式时，显示装置（6）就会结束显示显示由加密认证键盘所传送来的资料。本实施例的好处是利用原来计算机（9）的显示器作为显示装置（6），一般的计算机显示器内都设有处理器和记忆体等器件，只要在显示器内加设一个接口接收由加密认证键盘在保密模式下输出的资料就可以了，这样加密认证键盘就可以减省了设置显示屏的成本，而且计算机（9）的显示器的屏幕面积比较大，可以显示更多输入的资料。无论加密认证键盘的显示装置（6）采用本实施例的方式外接到计算机（9）显示器，或是采用前面各实施例的方式，都可很好地实现本发明的目的，都是属于本发明的保护范围。

参阅图 8，图 8 示出实施例可作进一步的改进，可以将电缆（601）合并到键盘电缆（401）和电缆（602）里，即在原来的键盘电缆（401）内增设多一组接线和接脚，同时在电缆（602）内也增设多这样的一组接线和接脚，这增设的一组接线和接脚就是原来电缆（601）的接线和接脚，然后通过计算机（9）将增设的一组接线和接脚从键盘接口连接到显示器接口，这样可减了加密认证键盘对外接线的电缆数量，虽然增设的一组接线和接脚

是通过计算机（9）才连接到显示器，但是这增设的一组接线和接脚与计算机（9）内部主板是物理上分离的，以保证安全。将电缆（601）合并到键盘电缆（401）和电缆（602）里，都可很好地实现本发明的目的，都是属于本发明的保护范围。

参阅图 9，图 9 是本发明的加密认证键盘的第九实施例的形像化立体示意图，本实施例与第八实施例相比，不同之处在于本实施例的加密认证键盘是设置在笔记本型计算机上，笔记本型计算机的显示屏就是加密认证键盘的显示装置（6），笔记本型计算机等于第八实施例中的计算机（9），加密认证键盘与计算机（9）是整合在一起的，如图 9 所示，加密认证键盘的各部件与计算机（9）和显示装置（6）组成笔记本型计算机，它们的操作方式和功能与第八实施例相同，都可很好地实现本发明的目的，都是属于本发明的保护范围。

本发明的加密认证键盘结构简单、操作容易、安全可靠、成本低廉，而且能有效对抗木马程式，保障一些通过终端机键盘输入的重要的资料能安全地传送到服务器，尤其适用于一些网上银行服务、服务股票交易等用途，也适合应用于一些涉及机密资料的服务器，它的实施，会带来良好的社会效益和经济效益。

权 利 要 求

1. 一种加密认证键盘，用于认证身份和加密资料，其特征在于，所述的加密认证键盘主要结构包括有主芯片（1）、键盘控制器（2）、按键（3）、通讯接口（4）、模式键（5）、显示装置（6），所述加密认证键盘，具有标准模式和加密模式，在标准模式下，在按键（3）上输入的资料会直接在通讯接口（4）输出，在加密模式下，在按键（3）上输入的资料会暂时保存在主芯片（1），输入完成后，按一次模式键（5）切换为标准模式时，主芯片（1）就会按预定程序提取一条未用的密钥（A）将暂存的资料加密，然后通过通讯接口（4）输出。

2. 如权利要求 1 所述的加密认证键盘，其中，主芯片（1）内设有 CPU 和存储器，并与键盘控制器（2）、通讯接口（4）、显示装置（6）等部件相连接，按预定程序运作，实现认证用户在服务器的身份和各项预定功能，包括将用户在加密模式下输入的资料加密、通过显示装置（6）显示提示信息、通过通讯接口（4）发送资料等，以及，键盘控制器（2）与各按键（3）及模式键（5）相连接，按预定程序运作，实现读取用户通过各按键（3）输入的资料，将用户输入的资料传送到主芯片（1）作进一步处理；

以及，

主芯片（1）将用户在加密模式下通过各按键（3）输入的资料，以密钥（A）将输入的资料加密，再通过通讯接口（4）传送给服务器，由服务器使用与该密钥（A）相配对的密钥（B）将资料解密还原出用户所输入

的资料，并核对资料内容，核对无误后表示用户的身份认证成功，然后服务器才会根据资料内容进行相应的操作。

3. 如权利要求 1 或 2 所述的加密认证键盘，其特征在于，所述的通讯接口（4）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、或 USB 接口、或 RS-232 接口、或 PS2 键盘接口。

4. 如权利要求 1 或 2 所述的加密认证键盘，其特征在于，所述的主芯片（1）内还包括有一个唯一的芯片编号（D）。

5. 如权利要求 1 或 2 所述的加密认证键盘，其特征在于，所述的主芯片（1）内设有多条密钥（A）和多个索引号（C），每一个索引号（C）对应一条密钥（A），以及，各个索引号（C）是互不相同的。

6. 如权利要求 1 或 2 所述的加密认证键盘，其特征在于，在加密模式下，用户在按键（3）上输入的资料会即时由键盘控制器（2）传送到主芯片（1），由主芯片（1）通过显示装置（6）即时将用户所输入的资料显示出来，并将所述的资料暂时保存在主芯片（1）内。

7. 如权利要求 1 所述的加密认证键盘，其特征在于，所述的模式键（5）主要用于选择主芯片（1）的工作模式，在标准模式下，当用户按一次模式键（5）后，主芯片（1）立即将工作模式切换为加密模式，以及，

当用户按一次模式键（5）后，主芯片（1）立即将工作模式切换为标准模式。

8. 如权利要求 1 或 2 或 7 所述的加密认证键盘，其特征在于，当所述的主芯片（1）内暂存的资料到达指定的大小时，或主芯片（1）的工作模式由加密模式切换为标准模式时，主芯片（1）会按预定程序从主芯片（1）内提取一条未用的密钥（A）和对应该密钥（A）的索引号（C），使用该密钥（A）将在加密模式下暂存的资料连同芯片编号（D）进行加密成为密文，然后将密文、索引号、芯片编号（D）等组成认证资料包，并将该认证资料包通过通讯接口（4）输出给服务器，以及，主芯片（1）将暂存的资料加密后，就会将暂存的资料删除，并将该条密钥（A）删除或弃置或标记为已用，使该条密钥（A）不会再次被主芯片（1）使用。

9. 如权利要求 8 所述的加密认证键盘，其特征在于，所述的加密认证键盘的结构还包括有储存装置接口（7），所述的储存装置接口（7）与外接的储存装置（8）相连接，主要用于将认证资料包通过储存装置接口（7）储存到外接的储存装置（8），以及，所述的储存装置（8）包括各类 USB 记忆装置、SD 记忆卡、Mini-SD 记忆卡、MMC 记忆卡、RS-MMC 记忆卡等记忆装置。

10. 如权利要求 1 或 2 或 7 所述的加密认证键盘，其特征在于，所述的主芯片（1）还设有开锁口令，在主芯片（1）的工作模式由标准模式切

换为加密模式前，用户必须通过按键（3）输入正确的开锁口令，主芯片（1）才将工作模式切换为加密模式。

11. 如权利要求 1 或 2 或 3 或 4 或 5 或 6 或 7 或 8 或 9 或 10 所述的加密认证键盘，其特征在于，所述的主芯片（1）主要结构包括有密钥卡（101）、接口电路（102）、连接器（103），其中，密钥卡（101）是单独的，与其它部件相隔开的部件，和接口电路（102）是通过连接器（103）相连接，接口电路（102）与键盘控制器（2）、通讯接口（4）、模式键（5）、显示装置（6）等部件相连接，密钥卡（101）内设有 CPU 和存储器、芯片编号（D）、多条密钥（A）和多个索引号（C）。

12. 如权利要求 11 所述的加密认证键盘，其特征在于，所述的连接器（103）可以是 USB 接口连接器、或 SD 记忆卡接口连接器、或 MINI-SD 记忆卡接口连接器、或 MMC 记忆卡接口连接器、或 RS-MMC 记忆卡接口连接器。

13. 如权利要求 11 所述的加密认证键盘，其特征在于，所述密钥卡（101）就是由金融机构发出的银行卡，包括各类信用卡、借记卡等银行卡，在支付时配合加密认证键盘使用。

14. 一种服务器，与加密认证键盘相配合，用于用户身份认证，其特征在于，所述的服务器内设有多个认证账户，每一个认证账户对应一个键盘的主芯片（1），认证账户内储存有该账户所对应的主芯片（1）的

芯片编号（D）和一个账户密码，每一认证账户内储存有多条密钥（B）和多个索引号（C），每一个索引号（C）对应一条密钥（B），

以及，

每一认证账户内的密钥（B）与该账户对应的主芯片（1）内的密钥（A）成配对关系，每一条密钥（B）有一条相配对的密钥（A），每一对相配对的密钥（A）和密钥（B）它们所对应的索引号（C）是相同的。

15. 如权利要求 14 所述服务器，其特征在于，所述的服务器每次接收到由键盘的主芯片（1）通过通讯接口（4）输出的认证资料包时，从认证资料包内容找出密文、索引号（C）、芯片编号（D），从芯片编号（D）在服务器内找到该芯片编号（D）对应的认证账户，从认证账户内提取一条与该索引号（C）对应对的密钥（B）将密文解密还原出用户所输入的资料及芯片编号（D），解密成功后核对芯片编号（D）无误后，服务器就可确认该认证资料包是从拥有该芯片编号（D）的主芯片（1）所发出的，以及，服务器将资料解密后，就会将该条密钥（B）删除或弃置或标记为已用，使该条密钥（B）不会再次被服务器使用。

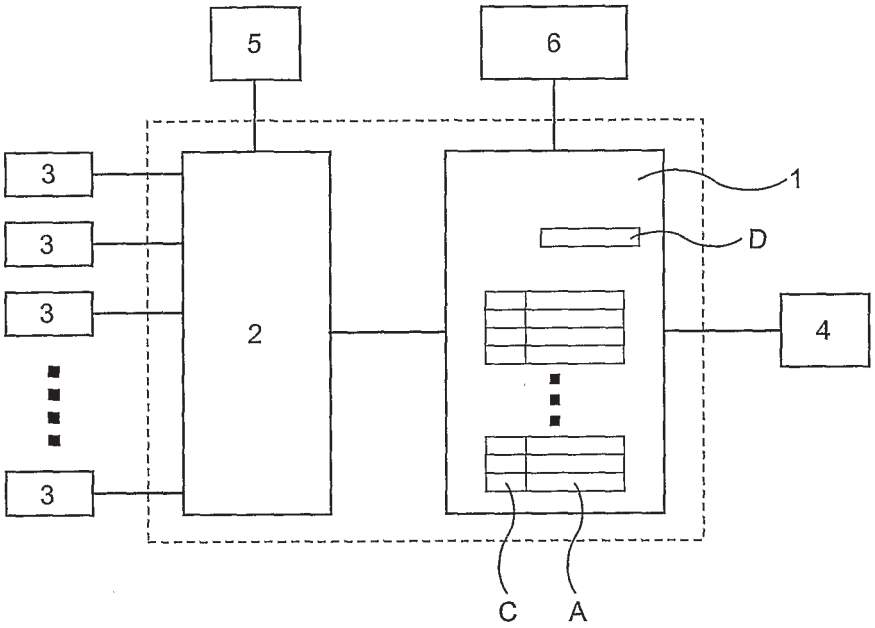

图 1

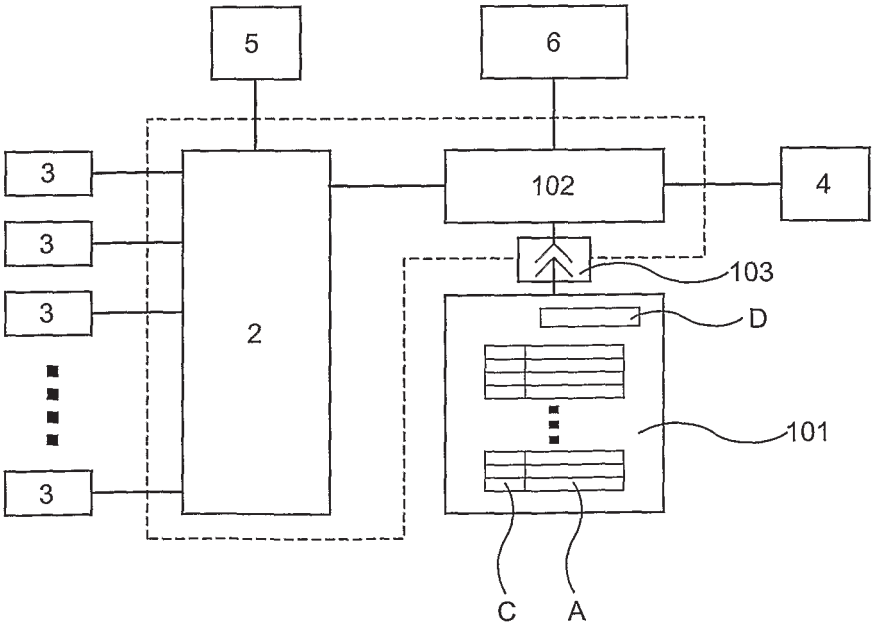

图 2

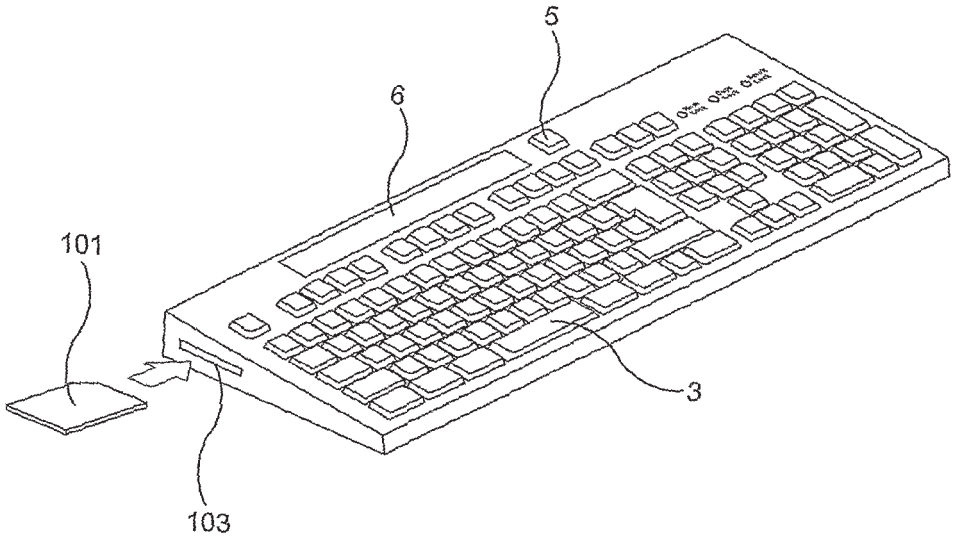

图 3

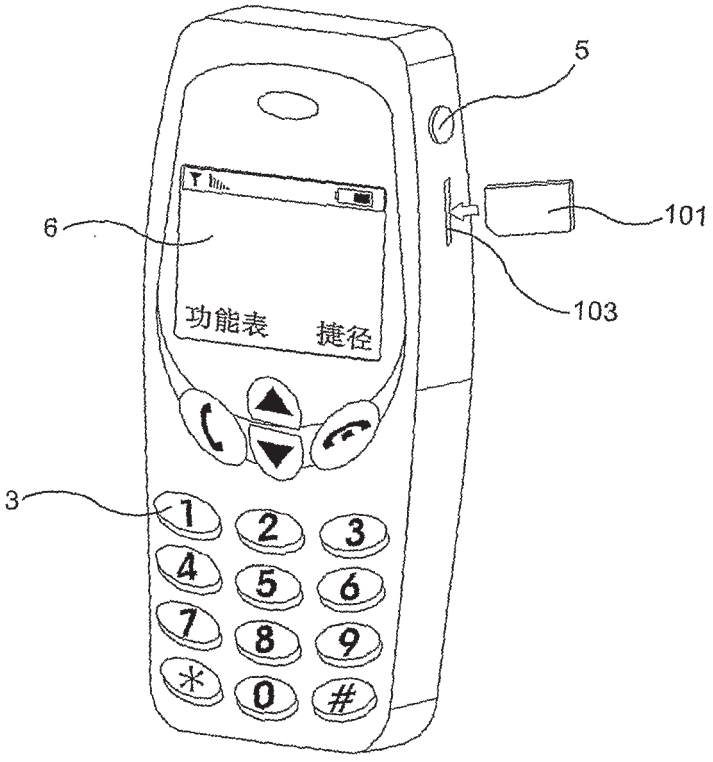

图 4

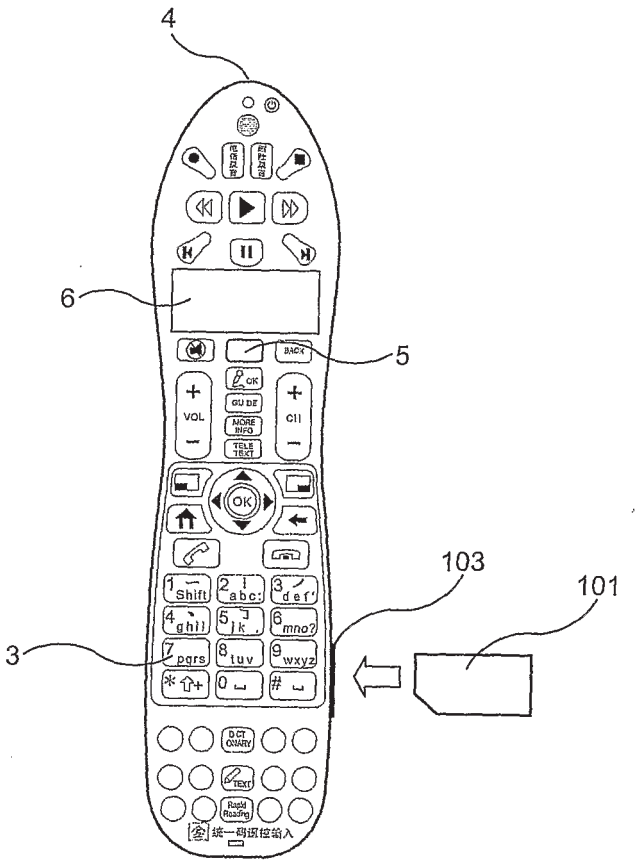

图 5

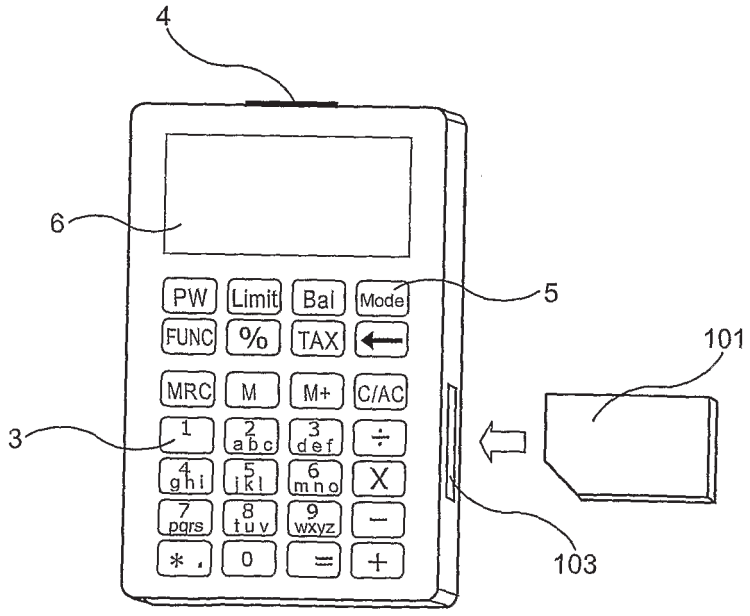

图 6

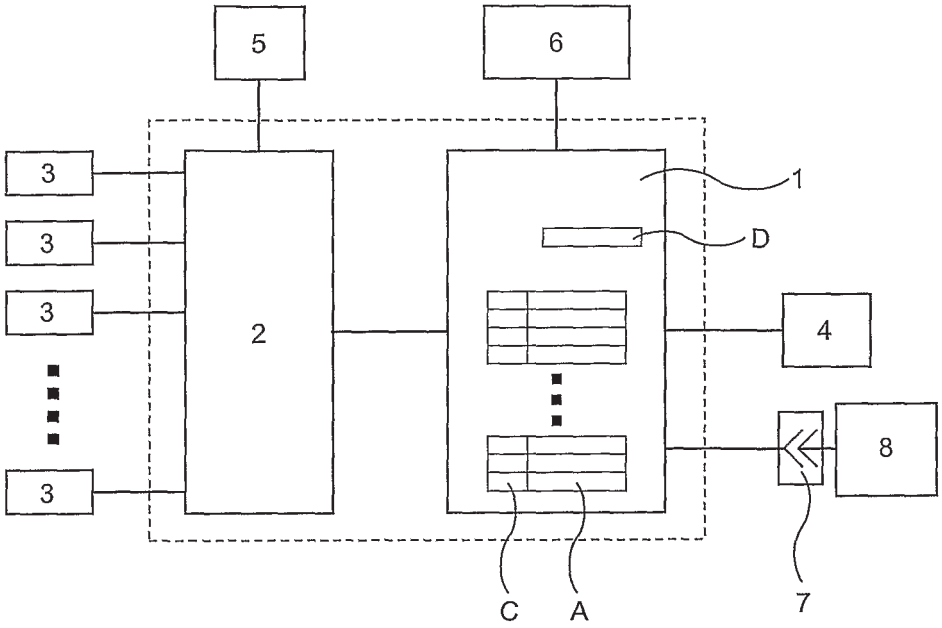

图 7

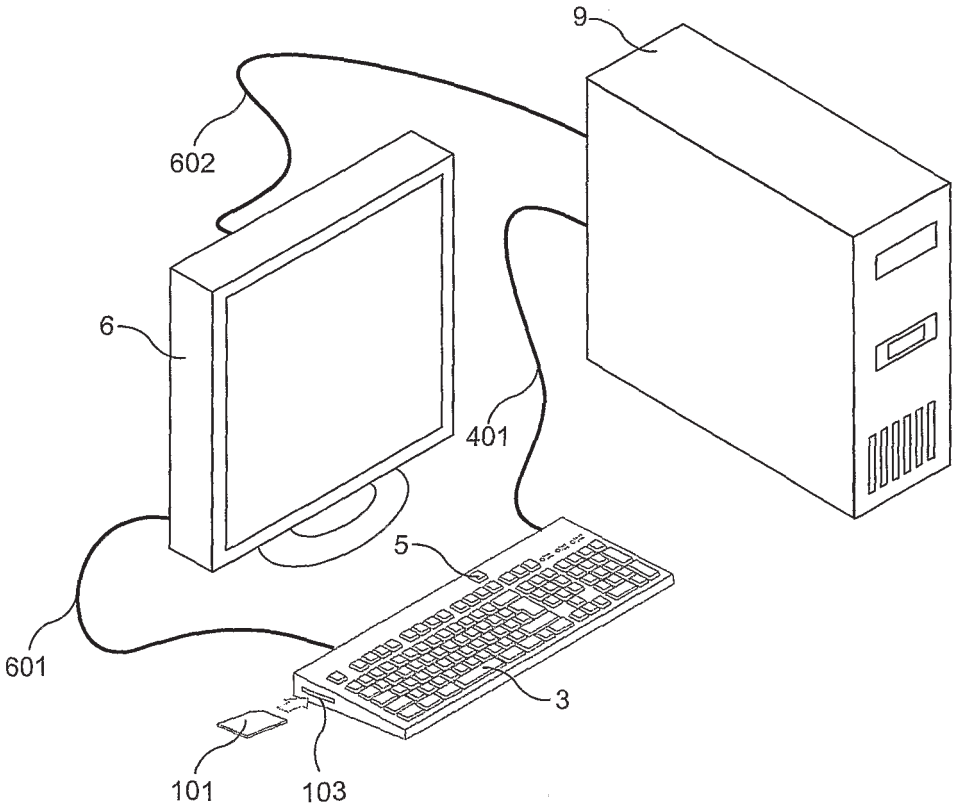

图 8

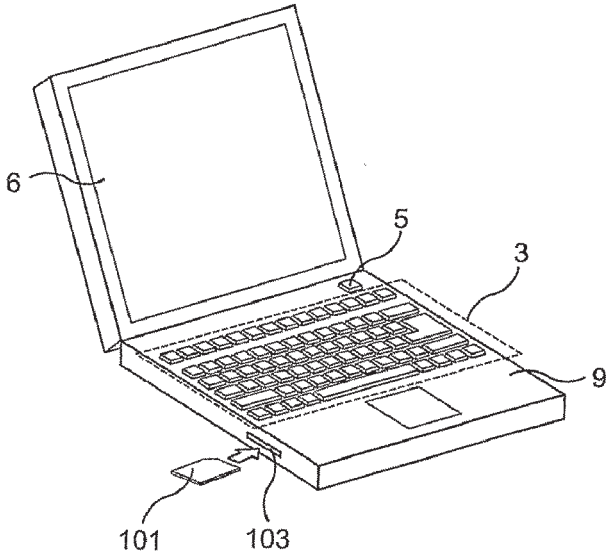

图 9