



(12) 发明专利申请

(10) 申请公布号 CN 102013981 A

(43) 申请公布日 2011. 04. 13

(21) 申请号 201010235186. 0

(22) 申请日 2010. 07. 23

(71) 申请人 杭州每日科技有限公司

地址 310013 浙江省杭州市西湖区文三路  
508 号天苑大厦 8 楼 D 座

(72) 发明人 方毅 俞锋锋 徐进

(74) 专利代理机构 浙江杭州金通专利事务所有  
限公司 33100

代理人 王雪

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/06(2006. 01)

G06Q 40/00(2006. 01)

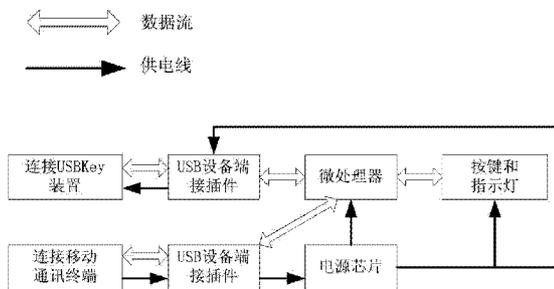
权利要求书 2 页 说明书 6 页 附图 6 页

(54) 发明名称

一种应用于移动通讯终端的网上银行数据认证装置及方法

(57) 摘要

本发明提供一种移动通讯终端的网上银行数据认证装置，它包括通讯模块、控制模块和供电模块，通讯模块与移动通讯终端、USBKey 相连，所述供电模块和控制模块相连，通讯模块和控制模块相连，控制模块包括微处理器。本发明还提供一种网上银行数据认证方法。它包括如下步骤：1) 将认证装置上的两个连接端分别与移动通讯终端和 USBKey 连接；2) 将移动通讯终端登录网上银行；3) 认证装置获得网上银行的交易信息，并将其传给 USBKey；4) USBKey 进行数字签名后，将签名数据通过连接端传递给前述认证装置，所述认证装置将签名数据传给移动通讯终端，将数据返回给网上银行系统，完成交易。本装置和方法能够提供手机和 USBKey 之间的实时的数据通讯连接，方便而且安全。



1. 一种移动通讯终端的网上银行数据认证装置,其特征在於它包括通讯模块、控制模块和供电模块,所述通讯模块与移动通讯终端、USBKey 相连,所述供电模块和控制模块相连,所述通讯模块和控制模块相连,所述控制模块包括微处理器。

2. 如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置,其特征在於它还包括加密模块,所述加密模块包括安装于移动通讯终端的加密 / 解密软件和安装于控制模块上、且与该软件相配套使用的解密 / 加密软件。

3. 如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置,其特征在於所述通讯模块包括两个连接端,所述两个连接端分别与移动通讯终端、USBKey 相连,所述通讯模块还包括数据传输装置以及通讯控制芯片。

4. 如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置,其特征在於所述供电模块包括电源芯片和 USB 设备端接插件。

5. 如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置,其特征在於所述供电模块包括电池和电源芯片。

6. 如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置,其特征在於所述微处理器和人机交互模块相连。

7. 一种移动通讯终端的网上银行数据认证方法,其特征在於它包括如下步骤:

1)、将权利要求 1 所述一种应用于移动通讯终端的网上银行数据认证装置上的两个连接端分别与移动通讯终端和 USBKey 连接;

2)、将移动通讯终端登录网上银行,录入网上银行的交易信息;

3)、如权利要求 1 所述一种应用于移动通讯终端的网上银行数据认证装置循环访问移动通讯终端,获得网上银行的交易信息,并将其传给 USBKey;

4)、USBKey 进行数字签名后,将签名数据通过连接端传递给如权利要求 1 所述一种应用于移动通讯终端的网上银行数据认证装置,所述认证装置将签名数据传给移动通讯终端,将数据返回给网上银行系统,完成交易。

8. 如权利要求 7 所述的一种移动通讯终端的网上银行数据认证方法,其特征在於它还包括加密步骤,所述加密步骤包括:

a)、在步骤 1) 时,在移动通讯终端上安装加密 / 解密软件,在如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置中安装与所述加密 / 解密软件相对应的解密 / 加密软件;

b)、在步骤 3) 时,所述移动通讯终端上的加密 / 解密软件对欲传递给 USBKey 的数据串进行加密并传递给如权利要求 1 所述的一种移动通讯终端的网上银行数据认证装置;

c)、所述认证装置上的解密 / 加密软件对所受到的数据串进行解密并传给 USBKey,并循环询问 USBKey 的反馈数据;

d)、所述认证装置获得步骤 3) 中的反馈数据并通过解密 / 加密软件进行加密后传给移动通讯终端;

e)、所述移动通讯终端上的加密 / 解密软件对所收到的、加密后的软件进行解密,并传给网上银行,交易成功。

9. 如权利要求 7 所述的一种移动通讯终端的网上银行数据认证方法,其特征在於它还包括确认用户身份步骤,所述确认用户身份步骤包括:

A)、在步骤 1) 时, 权利要求 1 所述一种应用于移动通讯终端的网上银行数据认证装置提示用户输入使用密码;

B)、在步骤 4) 时, USBKey 进行数字签名后, 将签名数据通过连接端传递给如权利要求 1 所述一种应用于移动通讯终端的网上银行数据认证装置时, 该装置再次提示用户输入使用密码;

C)、在步骤 4) 时, 将数据返回给网上银行系统, 完成交易时, 如权利要求 1 所述一种应用于移动通讯终端的网上银行数据认证装置提示用户进行最后确认。

## 一种应用于移动通讯终端的网上银行数据认证装置及方法

[0001]

### 技术领域

[0002] 本发明涉及一种移动通讯终端的网上银行数据认证装置及方法。

### 背景技术

[0003] 1996年中国银行首次将传统银行业务延伸到互联网。网上银行拥有低成本和价格优势,客户可以在任何时间、任何地方通过互联网就能得到银行的金融服务。发展到今天,国内几乎所有商业银行都推出自己的网上银行,同时网上银行的安全性也得到了发展和完善。目前网上银行大部分采用USBKey装置对客户进行身份认证。USBKey作为网上银行客户数字证书的载体,承担着保护客户数字证书和私有密钥安全性的重要责任,这对在网络上鉴别用户身份十分关键。其内部芯片操作系统特有的安全加密手段,高达1024位的非对称加密算法RSA,以及特殊的抗攻击方法,能确保客户在使用网络银行进行金融交易时,无需担心交易安全问题。同时,基于数字签名技术的这种网络金融服务可以提供有效的法律效力,所以目前在网络银行业务中,尤其是B2C业务中,银行越来越多地选择USBKey作为网络银行整体方案的基本硬件配置。USBKey使用时需要将其插入可以连接互联网的电脑,在进行网络交易时网络终端会将交易数据传入USBKey进行数字签名,然后校验签名结果,从而达到鉴别用户身份的目的。

[0004] 据中国工业和信息产业部的统计,截止到2009年底,全国共有手机用户74738.4万户,移动分组数据用户用38455.9万户,几乎一半的手机用户都会通过手机上网。随着手机上网的费用降低和手机自身技术的发展,手机接入互联网已经渐渐普及。

[0005] 手机用户通过手机浏览网页,查询信息,收发邮件,在线收看视频,或者登陆实时通讯软件。大部分在电脑上的互联网功能都已经能够在手机上实现。但是,缺少一种使用手机进行网络实时在线支付的功能。相对于个人电脑,手机在安全性上有着明显的缺陷。容易遗失,容易被人盗用,缺少外接接口都是造成迟迟不能在手机上实现在线支付功能的原因。

### 发明内容

[0006] 本发明所要解决的问题是提供一种方便移动通讯终端进行网上银行数据认证的移动通讯终端的网上银行数据认证装置,它包括通讯模块、控制模块和供电模块,所述通讯模块与移动通讯终端、USBKey相连,所述供电模块和控制模块相连,所述通讯模块和控制模块相连,所述控制模块包括微处理器。

[0007] 通过以上技术方案,本发明能方便移动通讯终端进行安全的网上数据认证。

[0008] 本发明还提供一种方便移动通讯终端进行网上银行数据认证的移动通讯终端的网上银行数据认证方法。它包括如下步骤:

- 1)、将前述一种应用于移动通讯终端的网上银行数据认证装置上的两个连接端分别

与移动通讯终端和 USBKey 连接；

2)、将移动通讯终端登录网上银行，录入网上银行的交易信息；

3)、前述一种应用于移动通讯终端的网上银行数据认证装置循环访问移动通讯终端，获得网上银行的交易信息，并将其传给 USBKey；

4)、USBKey 进行数字签名后，将签名数据通过连接端传递给前述一种应用于移动通讯终端的网上银行数据认证装置，所述认证装置将签名数据传给移动通讯终端，将数据返回给网上银行系统，完成交易。

[0009] 通过以上技术方案，本发明能够提供手机和 USBKey 之间的实时的数据通讯连接，方便而且安全。

[0010]

## 附图说明

[0011]

图 1 为本发明一种移动通讯终端的网上银行数据认证装置实施例 1 的原理框图。

[0012] 图 2 为本发明一种移动通讯终端的网上银行数据认证装置实施例 1 的结构示意图。

[0013] 图 3 为本发明一种移动通讯终端的网上银行数据认证装置实施例 1 使用过程中的网上银行数据流程示意图。

[0014] 图 4 为本发明一种移动通讯终端的网上银行数据认证装置实施例 1 的连接装置系统初始化通讯连接的流程图。

[0015] 图 5 为本发明一种移动通讯终端的网上银行数据认证装置的移动通讯终端软件流程图。

[0016] 图 6 为本发明一种移动通讯终端的网上银行数据认证装置实施例 1 进行数字签名通讯连接的流程图。

[0017] 图 7 为本发明一种移动通讯终端的网上银行数据认证装置实施例 2 的原理框图。

[0018] 图 8 为本发明一种移动通讯终端的网上银行数据认证装置实施例 2 的结构示意图。

[0019]

## 具体实施方式

[0020] 参见附图 1 和附图 2，本发明为一种移动通讯终端的网上银行数据认证装置，它包括通讯模块、控制模块和供电模块，所述通讯模块与移动通讯终端、USBKey 相连，所述供电模块和控制模块相连，所述通讯模块和控制模块相连，所述控制模块包括微处理器。

[0021] 本发明的移动通讯终端以手机为例，所述微处理器负责在移动通讯终端和 USBKey 装置之间建立安全的数据连接，该微处理器采用 ARM 芯片，ARM 微处理器是整个系统的控制、处理中枢。ARM 微处理器通过通讯模块，在预先烧制在 ARM 微处理器中的控制程序和握手协议控制下，与 USBKey 装置和手机进行通讯。除本实施例以外，本发明也可使用各种体系结构的微处理器，如单片微机或具备操作系统的处理器，本发

明的程序能跨平台编译，具有广泛的适应性和可移植性。

[0022] 所述通讯模块包括两个连接端，所述两个连接端分别与移动通讯终端、USBKey 相连，在本实施例中，两个连接端为两个 USB 接口，即所述通讯控制芯片上所设的 USB 主控接口和设备类接口。为了与此相配，所述通讯模块还包括 USB 设备端接插件，USB 主机端接插件和通讯控制芯片。

通讯模块是通讯信号的管理和控制模块，可以是独立的 USB 通讯控制芯片，管理和控制本发明与移动通讯终端和 USBKey 装置的数据通讯。在实际操作中，也可以集成在微处理器上。通讯控制芯片是通讯模块的主要部分，当微处理器自身具有 USB 主控接口或设备类接口时，可以采用单独的 USB 设备类通讯芯片或者单独的 USB 主控通讯芯片。如果微处理器同时具有 USB 主控接口和设备类接口时，可不设置此 USB 通讯芯片。本实施例的通讯模块采用微处理器本身具备的通讯接口。

[0023] 所述通讯模块内不存在存储芯片或存储介质，通讯模块芯片和数据传输装置只负责提供实时的数据通讯连接，不会保存和泄漏 USBKey 装置中的任何信息。

[0024] 在本实施例中，所述供电模块包括电源芯片和 USB 设备端接插件。使用时，USB 设备接插件需要连接移动通讯终端。电源芯片通过 USB 设备端接插件获得电源，经过稳压，滤波，变压之后，为其他所有模块提供电源。当微处理器芯片自身具备变压和滤波等功能模块时，可以不采用单独的电源芯片，直接使用微处理器芯片为自身和其他所有模块提供电源。本实施例的通讯模块采用单独的电源芯片。

[0025] 在本实施例中，所述微处理器还和人机交互模块相连。人机交互模块可以提供对本发明进行控制的接口，比如按键。同时也提供本发明工作状态的指示接口，比如通过指示灯或液晶屏显示本发明的工作状态等信息。

[0026]

本发明一种移动通讯终端的网上银行数据认证装置还包括加密模块。所述加密模块包括安装于移动通讯终端的加密/解密软件和安装于控制模块上、且与该软件相配套使用的解密/加密软件。所述两个加密软件相互呼应，使得传输的数据避免被窃取的可能。所述安装于移动通讯终端的加密/解密软件可以从属于网上银行登录和支付软件，也可以单独安装。该软件安装在移动通讯终端上，用于控制 USBKey 数据的读取以及加密信息和网上银行服务器之间的通信。

[0027] 控制模块同时管理本发明支持的移动通讯终端和 USBKey 装置的型号。控制模块还可以包括外围时钟电路、测试电路等。

[0028]

参见附图 3 和附图 5。附图 3 显示了本发明连接移动通讯终端和 USBkey，进行网上银行认证时的数据流。附图 5 显示了本发明移动通讯终端软件的流程图。本发明使用的时候，移动通讯终端先将浏览器接入网上银行服务器（即用移动通讯终端登录手机网上银行），然后本发明在移动通讯终端上安装的加密/解密软件，自动激活启动，由网上银行服务器发送认证数据串 A，所述认证数据串 A 通过移动通讯终端的加密/解密软件进行加密，加密后的认证数据串 A 通过本发明与移动通讯终端之间的 USB 接口输入，通过本发明内置的 USB 设备端接插件后输入控制模块的微处理器。同时，安装于移动通讯终端的加密/解密软件开始等待本发明将加密后的数据返回。如果等待数据返回超时，则自动

退出此次操作，并通过移动通讯终端屏幕提示数据认证失败。由于本发明软件包含 USB 通讯协议和 USB 设备自动识别程序，本发明能够自动通过该协议连接手机和 USBKey 装置，不需要用户进行设置和操作。

[0029] 然后，微处理器通过内置的解密软件（即前述安装于控制模块上、且与该软件相配套使用的解密 / 加密软件）将其解密，然后通过 USB 设备端接插件，通过另一个与 USBKey 连接的 USB 接口，输入到 USBKey 里进行数字签名。这样就完成了一个加密和解密的步骤，使得所传输的数据不会被窃取。

[0030] 从 USBKey 里输出的认证数据串 B 重复类似但是步骤相反的步骤，在微处理器内进行加密后，在移动通讯终端的解密 / 加密软件进行解密。具体来说，移动通讯终端判断，是否在规定时间内，收到由本发明的数据返回，然后将收到的认证数据串 B 解密，解密后校验是否正确，再将解密后的认证数据串 B 发送给网上银行服务器，等待网上银行服务器发送验证信息返回，如果网上银行服务器回复认证成功，则认证过程成功，反之失败。

[0031] 微处理器在整个过程中会通过按键和指示灯实时显示认证状态，并接收用户的按键终止操作。

[0032] 本发明内置唯一出厂唯一序列号，用于上位机软件识别客户信息。通讯加密方式可以是普通的对称加密，也可以是非对称加密。

[0033]

参见附图 6。附图 6 显示了本发明进行数字签名通讯连接的流程图。本发明的工作过程为：首先，本发明循环检测移动通讯终端发送的数据，在收到移动通讯终端发送的待签名认证数据串后为其解密和校验，解密后判断其是否是有效认证数据串，然后发送到 USBKey 装置，并等待 USBKey 装置进行回馈，并在收到 USBKey 装置发回的签名后的认证数据串后，对收到的认证数据串进行加密，并将加密后的认证数据串发回移动通讯终端，等待移动通讯终端进行解密，从而数字签名成功。如果等待认证数据串返回超时，则自动退出此次操作，并通过指示灯显示。如果本发明在规定的时间内接收到 USBKey 装置发回的认证数据串，则将认证数据串加密后发送回移动通讯终端，并显示签名成功。

[0034] 本发明的工作过程还包括对用户身份进行确认的步骤，具体来说，本发明的控制芯片内置密码输入程序，在本发明与移动通讯终端和 USBKey 相连初始，本发明提示用户输入密码，当签名发送回移动通讯终端，交易即将完成时，本发明再次提示用户输入密码，并可重复要求输入两遍，当交易完成时，本发明会弹出：“交易完成”确认窗口。

[0035]

参见附图 4。附图 4 显示了本发明连接移动通讯终端和 USBKey 装置时的流程图。本发明的初始化使用过程为，先将本发明接入移动通讯终端系统获得电源之后进行初始化。

[0036] 系统初始化成功之后，配置 USB 通讯协议，连接移动通讯终端，判断是否支持该移动通讯终端，如果是的话继续下一步，否的话本发明的人机交互界面提示系统出错。

[0037] 如果是的话再确认下一步，是否与该移动通讯终端通讯连接成功。接入成功后，接入 USBKey 装置，然后再确认是否与该 USBKey 装置通讯成功，最后由本发明的指示灯提示，通讯建立成功。当系统与移动通讯终端和 USBKey 装置均建立通讯连接之后，本发明通过指示灯提示系统连接成功，反之则提示失败。从而完成了本发明的初始化。

[0038]

本发明所解决的另一个技术问题是，当本发明的通讯模块通过 USB 接口连接 USBKey 和移动通讯终端时，本发明均属于主机，本发明的两个接口均为主机口，而当本发明的通讯模块连接电脑时，本发明属于从机，本发明的接口自动转换为从机口。这是由于本发明内置对接口的电平检测装置所判断的。当本发明的控制模块判断对方为从机时，该控制模块会不断发出指令，从而跟 USBKey 和移动通讯终端取得信号连接。而当本发明判断对方为主机（电脑）时，本发明的接口自动转换为从机口。

[0039] 本实施例的通讯模块里，是不设存储空间的，也就是说，数据是“不落地”的，最大限度的保证了安全。而本发明的控制模块里，设有专门用于软件升级和安装的存储区间。因此，本发明能够通过 USB 接口接入电脑，可以作为虚拟可移动磁盘，通过存入升级文件的方式对所述装置支持的移动通讯终端和 USBKey 装置的数量和型号进行升级和配置，也可以将所述装置作为特殊 USB 设备，使用专用软件对所述装置支持的移动通讯终端和 USBKey 装置的数量和型号进行升级和配置。

[0040]

#### 实施例 2

参照附图 7，8。本实施例 2 和实施例 1 基本相同。在本实施例中，本发明的供电模块包括了电池和电源芯片。本发明不再从移动通讯终端获取电源，而是通过电池进行供电。也就是说，本发明可以通过手机供电进行工作，也可以通过附带电池或者外接输入电源工作。当本发明附带电池或者外接输入电源时，本发明可以同时为手机进行充电。

[0041] 也就是说，本发明的供电模块可以是独立的电源模块，供电方式为电池供电，供电模块控制和转换电池电压，为控制模块、通讯模块和人机交互模块提供所需的电压。供电模块也可以是从移动通讯终端获取电能，控制和转换电压后，为控制模块，通讯模块和人机交互模块提供所需的电压。供电模块同时负责保障供电安全性，能够杜绝短路过流，输入过压对本发明其他模块的损害。

[0042]

实现各功能的工作过程与实施例 1 相同。

[0043] 为了网上银行的安全性和使用电脑进行网上支付的通用性，本发明提出的移动通讯终端网上银行数据认证方法仍然使用通用的 USBKey 装置。本发明提供一个能够同时连接 USBKey 装置和移动通讯终端的附件。移动通讯终端连接互联网进行网上银行交易时，该附件能够提供手机和 USBKey 之间的实时的加密数据通讯连接。同时本发明提供了安装于不同移动通讯终端的加密 / 解密软件。

[0044] 本发明连接手机的 USB 端接口可以是带或者不带延长线的 USB 插头，封装形式可以是 mini USB、micro USB、USB A 型插头或者 USB A 型或 B 型插座。当该 USB 接

口为 USB A 型或 B 型插座时，设备可以连接通讯终端所配的数据线，这类数据线可以是标准 USB A 型或 B 型插头转 mini USB B 型插头的数据线，也可以是针对不同通讯终端设备的接口定制的固定的或者可以更换的不同接口形状的单头或者多头的连接端口，以此支持不同厂商的不同通讯接口。

[0045]

本发明还提供一种应用于移动通讯终端的网上银行数据认证方法，它包括如下步骤：

1)、将前述一种应用于移动通讯终端的网上银行数据认证装置上的两个连接端(USB 端口)分别与移动通讯终端和 USBKey 连接。

[0046] 2) 将移动通讯终端登录网上银行，录入网上银行的交易信息。

[0047] 3) 前述一种应用于移动通讯终端的网上银行数据认证装置循环访问移动通讯终端，获得网上银行的交易信息，并将其传给 USBKey。

[0048] 4) USBKey 进行数字签名后，将签名数据通过连接端传递给前述一种应用于移动通讯终端的网上银行数据认证装置，所述认证装置将签名数据传给移动通讯终端，将数据返回给网上银行系统，完成交易。

[0049]

它还包括加密步骤，所述加密步骤包括：

a)、在步骤 1) 时，在移动通讯终端上安装加密/解密软件，在前述的一种移动通讯终端的网上银行数据认证装置中安装与所述加密/解密软件相对应的解密/加密软件；

b)、在步骤 3) 时，所述移动通讯终端上的加密/解密软件对欲传递给 USBKey 的数据串进行加密并传递给前述的一种移动通讯终端的网上银行数据认证装置；

c)、所述认证装置上的解密/加密软件对所收到的数据串进行解密并传给 USBKey，并循环询问 USBKey 的反馈数据；

d)、所述认证装置获得步骤 3) 中的反馈数据并通过解密/加密软件进行加密后传给移动通讯终端；

e)、所述移动通讯终端上的加密/解密软件对所收到的、加密后的软件进行解密，并传给网上银行，交易成功。

[0050]

它还包括确认用户身份步骤，所述确认用户身份步骤包括：

A)、在步骤 1) 时，前述一种应用于移动通讯终端的网上银行数据认证装置提示用户输入使用密码；

B)、在步骤 4) 时，USBKey 进行数字签名后，将签名数据通过连接端传递给前述一种应用于移动通讯终端的网上银行数据认证装置时，该装置再次提示用户输入使用密码；

C)、在步骤 4) 时，将数据返回给网上银行系统，完成交易时，如前述一种应用于移动通讯终端的网上银行数据认证装置提示用户进行最后确认。

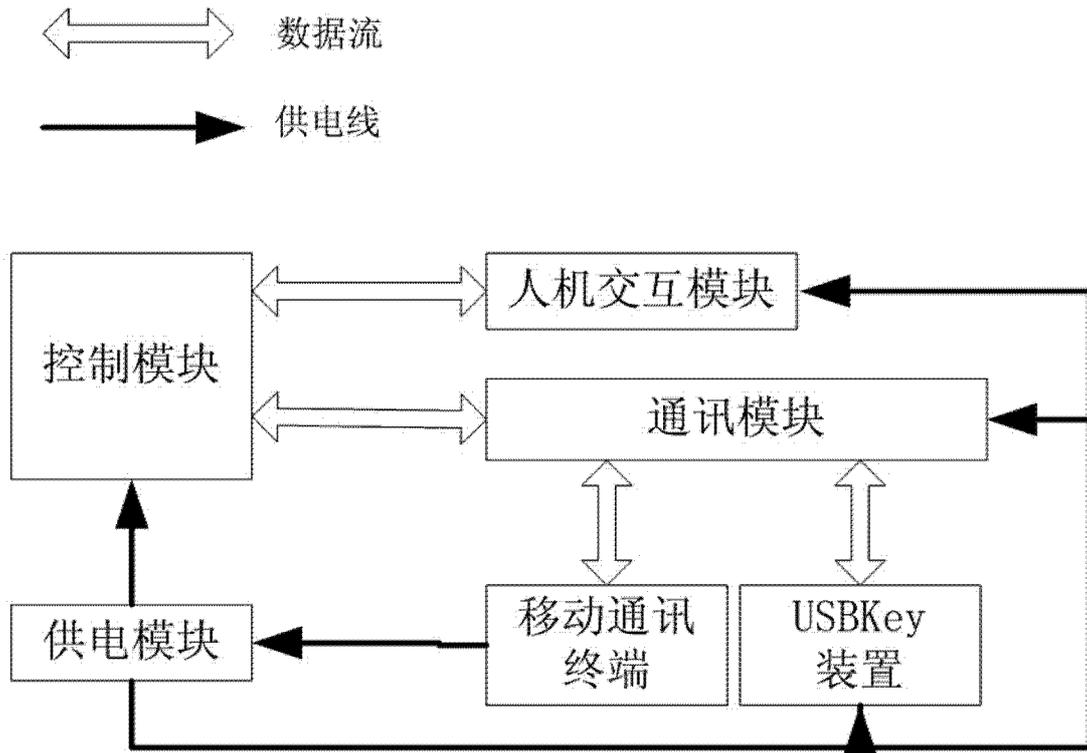


图 1

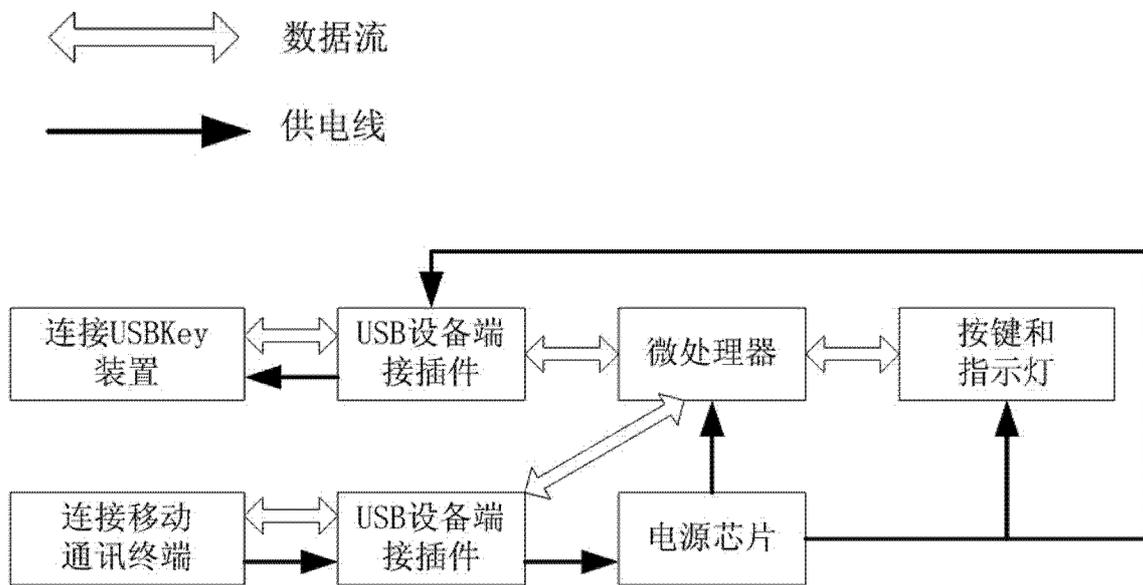


图 2

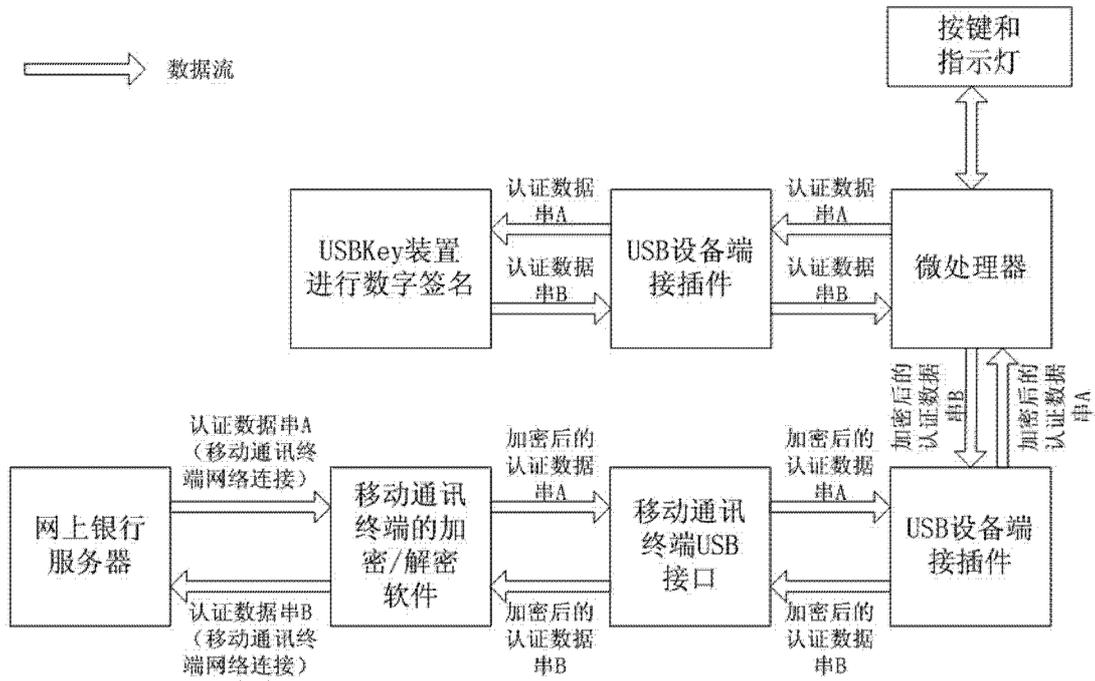


图 3

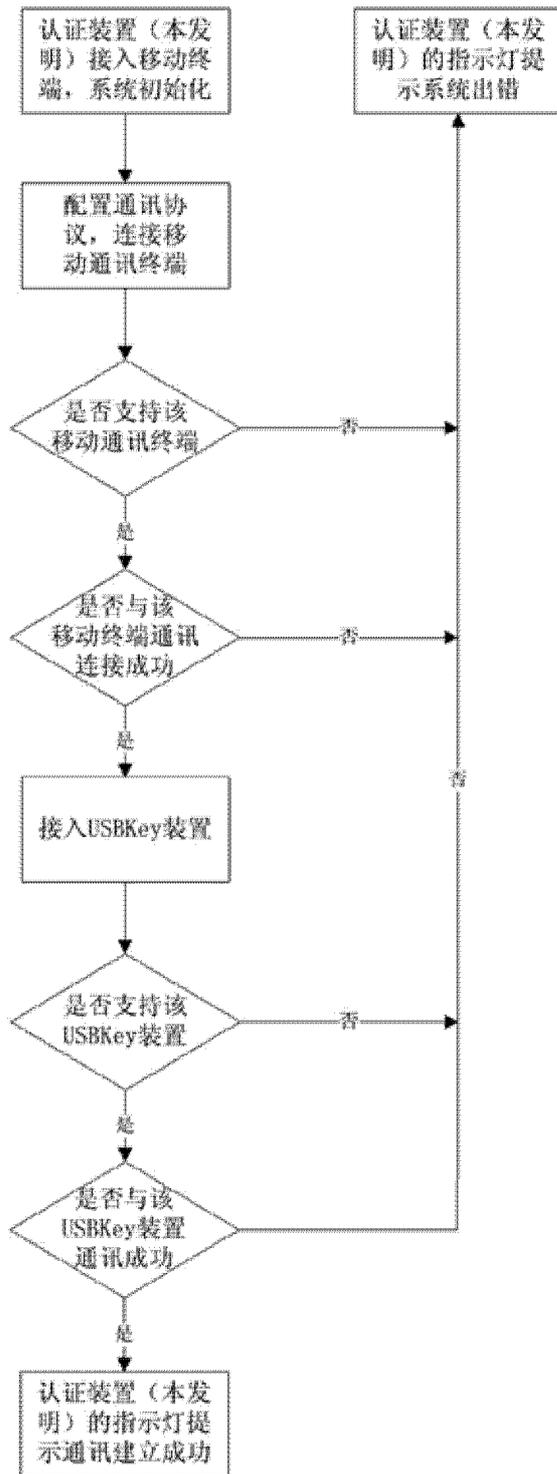


图 4

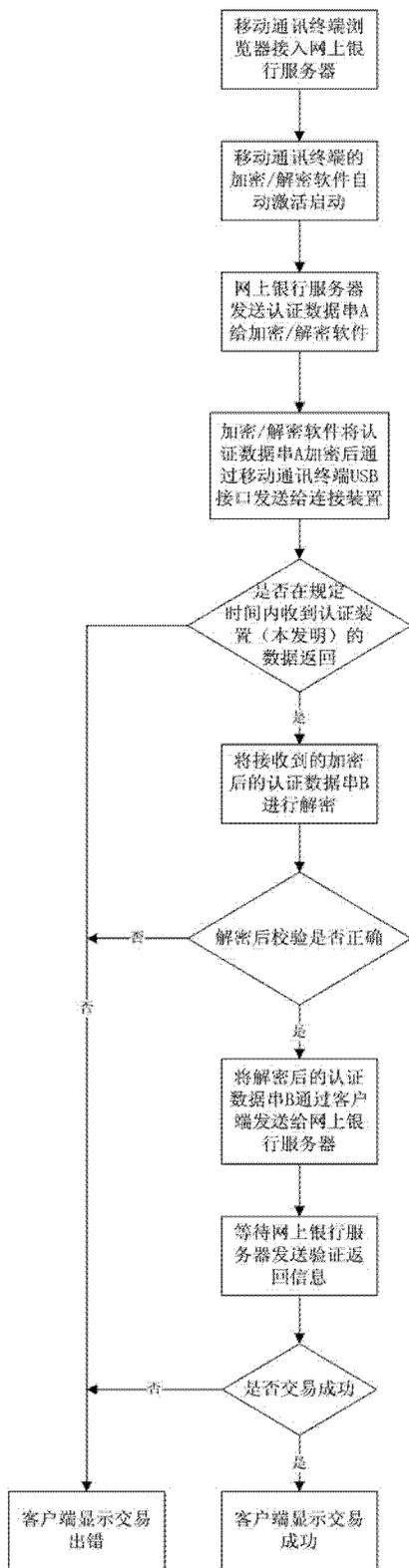


图 5

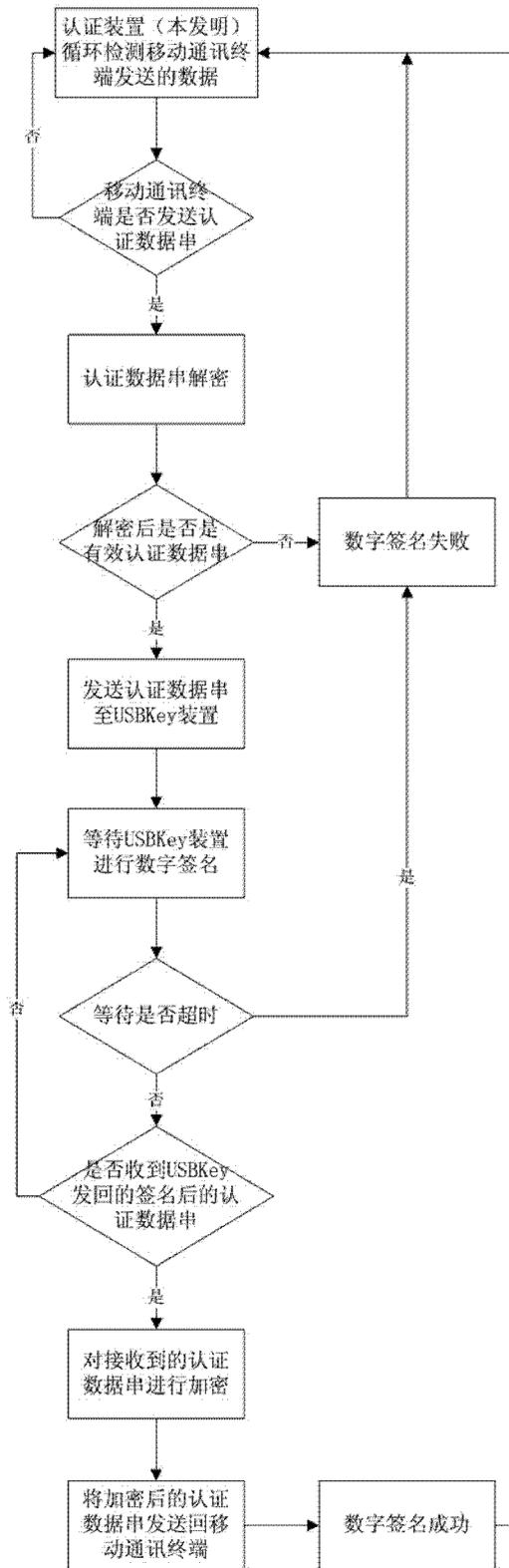


图 6

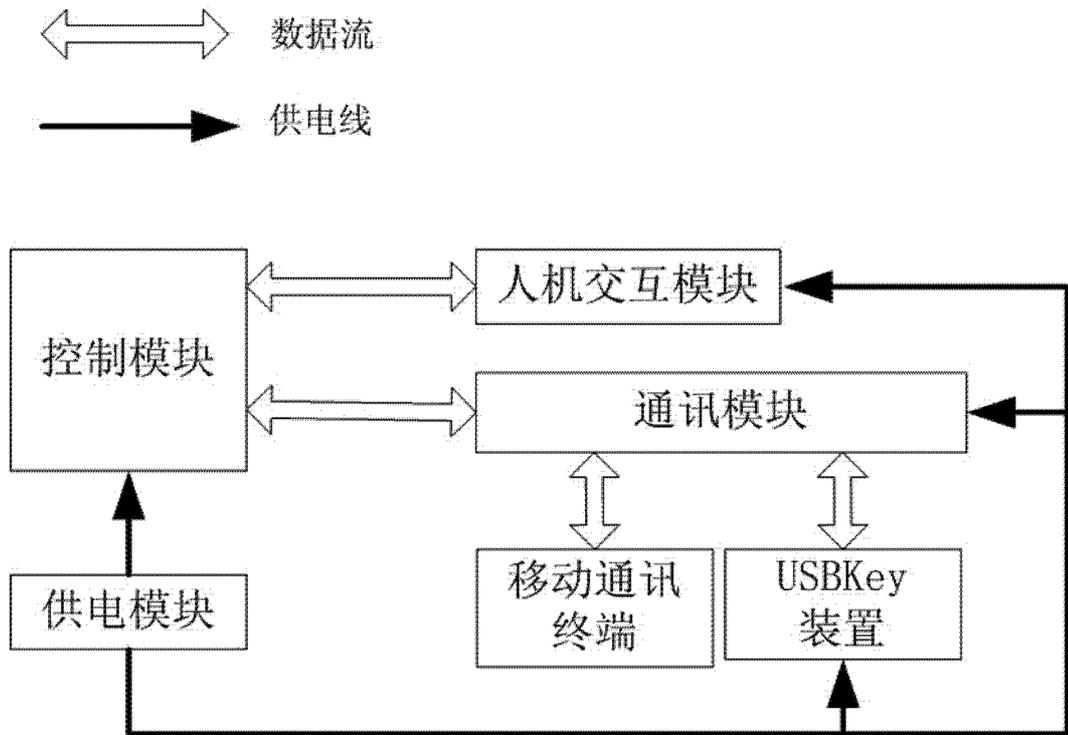


图 7

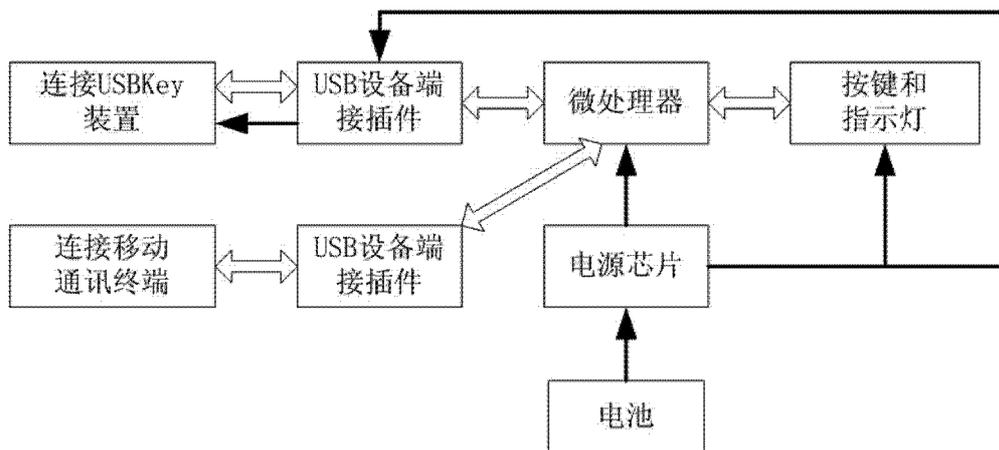


图 8