[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06K 9/62 (2006.01)*
*G06F 17/00 (2006.01)*
*G06F 13/00 (2006.01)*

[12] 发明专利说明书

专利号 ZL 03100326.5

[45] 授权公告日 2009 年 5 月 27 日

[11] 授权公告号 CN 100492402C

[22] 申请日 2003.1.9 [21] 申请号 03100326.5

[73] 专利权人 北京握奇数据系统有限公司

地址 100102 北京市朝阳区望京中环南路 9 号望京大厦 B 座 18 层

[72] 发明人 陈大才 邹恒泰 彭志宽

[74] 专利代理机构 北京三友知识产权代理有限公司

代理人 李 强

[56] 参考文献

JP2000－285065A 2000.10.13

CN1304115A 2001.7.18

US6385677B1 2002.5.7

EP1174820A1 2002.1.23

CN2414460Y 2001.1.10

CN1312516A 2001.9.12

审查员 许菲菲

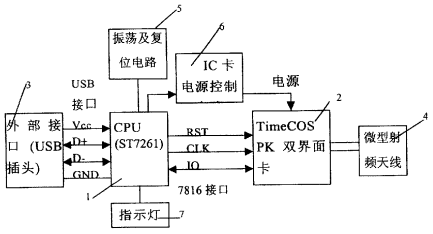
权利要求书 1 页 说明书 5 页 附图 2 页

[54] 发明名称

# 双界面电子钥匙

[57] 摘要

一种双界面电子钥匙，包括：一 CPU 芯片、一双界面 PK 卡、一 USB 接口、一微型射频天线和外围电路；所述 CPU 芯片与 USB 接口相连接，并与双界面 PK 卡通过 ISO7816 标准接口连接，所述双界面 PK 卡通过射频接口与微型射频天线连接，所述外围电路产生振荡信号、复位信号及电源控制信号，用以控制所述 CPU 芯片和双界面 PK 卡；由于本发明不仅具有 USB 接口，而且具有射频接口，在非接触状态下可直接与外部射频读写器进行通讯，因而使用方便快捷；由于本发明采用双界面 PK 卡，支持 1024 位 RSA 密码算法，支持卡内密钥生成、加密、解密、签名、验证。



1、一种双界面电子钥匙，其特征在于包括：一 CPU 芯片、一双界面公开密钥算法卡、一 USB 接口、一微型射频天线和外围电路；所述 CPU 芯片与 USB 接口相连接，并与双界面公开密钥算法卡通过 ISO7816 标准接口连接，所述双界面公开密钥算法卡通过射频接口与微型射频天线连接，所述外围电路产生振荡信号、复位信号及电源控制信号，用以控制所述 CPU 芯片和双界面公开密钥算法卡。

2、如权利要求 1 所述的双界面电子钥匙，其特征在于：所述公开密钥算法卡内部包括以下功能模块：CPU、随机存储器、只读存储器、高级加密引擎、双钥及椭圆密码算法模块、随机数发生器、循环冗余校验码模块、定时器、通用异步收发器模块、中断控制模块、安全保护模块、射频接口模块以及 7816 物理接口，各模块之间提供总线相互连接。

3、如权利要求 1 或 2 所述的双界面电子钥匙，其特征在于：所述外围电路包括振荡电路、复位电路及 IC 卡电源控制电路；所述振荡及复位电路与 CPU 芯片电连接，所述 IC 卡电源控制电路的输入端与 CPU 芯片电连接，输出端与双界面公开密钥算法卡电连接，用以提供该双界面公开密钥算法卡的工作电源。

4、如权利要求 1 或 2 所述的双界面电子钥匙，其特征在于：所述外围电路还包括有工作指示灯电路；

5、如权利要求 1 或 2 所述的双界面电子钥匙，其特征在于：所述射频接口为符合 ISO14443 协议的 A、B 兼容的射频接口。

6、如权利要求 5 所述的双界面电子钥匙，其特征在于：所述双界面公开密钥算法卡的内部操作系统为符合中国人民银行标准的实时操作系统。

7、如权利要求 1、2 或 6 所述的双界面电子钥匙，其特征在于：所述 USB 接口包括两条信号线和两条电源线。

# 双界面电子钥匙

## 技术领域

本发明涉及电子信息系统的身份识别领域，尤指一种支持非对称密钥算法的双界面电子钥匙。

## 背景技术

目前，现有的类似产品一般由微型读写器和通用 IC 卡整合在一起而形成，对外接口为 USB 接口。其主要特点是：USB 接口，即插即用；集成 CPU 智能卡，技术上与 IC 卡完全一致，其身份标识、电子签名等信息受 IC 卡内 CPU 保护或由 IC 卡内 CPU 产生，外部无法获取；而且该产品可作为 IC 卡直接在计算机上使用，带来可信赖的安全特性。

但是，目前这类产品不支持非对称密钥算法。

另外，产品与计算机的连接，由 USB 接口插头与计算机 USB 接口插座或其转接线的插座相连，这一点易导致接触不良或连接太紧，不方便插拔。

## 发明内容

鉴于上述，本发明提供一种功能更强、使用更方便灵活的支持非对称密钥算法的双界面电子钥匙。

本发明的双界面电子钥匙包括：

一 CPU 芯片、一双界面 PK（公开密钥算法，Public Key algorithm）卡、一 USB 接口、一微型射频天线和外围电路；所述 CPU 芯片与 USB 接口相连接，并与双界面 PK 卡通过 ISO7816 标准接口连接，所述双界面 PK 卡通过射频接口与微型射频天线连接，所述外围电路产生振荡信号、复位信号及电源控制信号，用以控制所述 CPU 芯片和双界面 PK 卡。

根据上述方案，所述 PK 卡内部包括以下功能模块：CPU、随机存储器、只读存储器、高级加密引擎、双钥及椭圆密码算法模块、随机数发生器、循环冗余校验码模块、定时器、通用异步收发器模块、中断控制模块、安全保护模块、射频接口模块以及 7816 物理接口，各模块之间提供总线相互连接。

所述外围电路包括振荡电路、复位电路及 IC 卡电源控制电路；所述振荡及复位电路与 CPU 芯片电连接，所述 IC 卡电源控制电路的输入端与 CPU 芯片电连接，输出端与双界面 PK 卡电连接，用以提供该双界面 PK 卡的工作电源。

所述外围电路还包括有工作指示灯电路。

所述射频接口为符合 ISO14443 协议的 A、B 兼容的射频接口；

所述双界面 PK 卡的内部操作系统为符合 PBOC（中国人民银行）标准的实时操作系统（TimeCOS）。

所述 USB 接口包括两条信号线和两条电源线。

本发明相对现有技术而言，具有如下优点：

1、由于本发明不仅具有 USB 接口，而且具有射频接口，在非接触状态下可直接与外部射频读写器进行通讯，因而使用方便快捷。

2、本发明采用双界面 PK 卡，支持 1024 位非对称密钥算法，支持卡内密钥生成、加密、解密、签名、验证，同时支持 3DES 以及国密办指定的国产加密算法 SSF33。

3、本发明内附符合 CSP、PKCS#11 规范的软件接口，能实现加密解密、证书管理和高度安全的 SSL 通讯功能，故能为用户端提供在 Internet 和 Intranet 上的安全通信，实现与浏览器的无缝连接，并且支持访问安全网站、加密邮件传送和对表单进行签字等功能。

附图说明

图 1 为本发明的结构框图;

图 2 为双界面 PK 卡内部结构框图;

图 3 为本发明的电路图。

具体实施方式

图 1 为本发明的结构框图。如图 1 所示，本发明的双界面电子钥匙包括一 CPU 芯片 1、一双界面 PK 卡 2、一 USB 接口 3、一微型射频天线 4 和外围电路；所述外围电路又包括振荡及复位电路 5、IC 卡电源控制电路 6 和工作指示灯电路 7。

在本实施例中选用 ST 公司的 ST7261 CPU 芯片，其信号线(D+、D-)和电源线(Vcc、GND)引到 USB 插头即构成对外 USB 输出接口 3。所述双界面 PK 卡 2 与 ST7261 芯片 1 之间为符合 ISO7816 的标准接口，其中，时钟信号 CLK 从 ST7261 芯片 1 输出到双界面 PK 卡 2；输入输出信号 IO 为 ST7261 芯片 1 与双界面 PK 卡 2 之间双向传输；复位信号 RST 从 ST7261 芯片 1 输出到双界面 PK 卡 2；该双界面 PK 卡与微型射频天线 4 连接共同组成符合 ISO14443 协议的 A、B 兼容射频接口，可与符合该标准的射频读写器进行通讯，完成数据交换；所述振荡及复位电路 5 与 ST7261 芯片 1 电连接，为 ST7261 芯片 1 提供振荡信号及复位信号； 所述 IC 卡电源控制电路 6 的输入端与 ST7261 芯片 1 电连接，输出端与双界面 PK 卡 2 电连接，用以提供该双界面 PK 卡 2 的工作电源；所述指示灯电路 7 与 ST7261 芯片 1 电连接，用以显示该 ST7261 芯片 1 的工作状态。

图 2 为双界面 PK 卡的结构图，如图 2 所示，所述双界面 PK 卡包括以下功能模块：CPU、RAM、ROM、高级加密引擎 ACE（Advanced Crypto Engine）、双钥及椭圆密码算法模块 DDES-EC2（Dual Key DES and Elliptic Cueve Accelerator）、随机数发生器 RNG（Random Number Generatot）、循环冗余校验模块 CRC（Cyclic Redundance Check）、定时器 Timer、通用

异步收发器模块 UART（Universal Asynchronous Receiver Transmitter）、中断控制模块、安全保护模块、射频接口模块及 7816 物理接口，各模块之间通过总线相互连接。所述双界面 PK 卡从功能和结构上讲，实际上是一个微型计算机系统，该系统具有符合 ISO7816 标准的物理接口和符合 ISO14443 标准的射频接口。

双界面PK卡内操作系统为符合PBOC标准的TimeCOS，支持1024位RSA密码算法。RSA算法是以M.I.T的R.L. Rivest，A. Shamir 和 L .Adleman 三人名中的首字母命名的公钥算法系统，其原理基于上述三人发表的文献“On Digital signatures and Public Key Cryspto System”（Communications of the ACM，Vol. 21，no. 2，pp. 120-125，1978.），该算法的原理为：

首先，选择密钥：选择两个足够大的素数p和q，且令：

$n = p * q;$

其中n为1024位，可公开，但p和 q 保密，计算偶拉函数：

$\phi(n) = (p-1) * (q-1)$

任选一个与中 $\phi(n)$互素的整数 e 作为公开的加密密钥，解密密钥 d（需要保密）满足：

$d * e = 1 \bmod(\phi(n))$

亦即：$d * e = k * (p-1) * (q-1)+1$

上式中，整数 k 是$(p-1)$和$(q-1)$的最大公约数。

这样，(e, n)和(d, n)就分别是加密密钥和解密密钥。

然后；可进行加密和解密：

加密前，先将欲加密的报文M数字化，即变换为0~(n－1)间的数，如果M较长，则应将M分为长度小于logn的若干组，逐组进行以下加密运算：

$c_i=E(m_i)=m_i^e \bmod(n)$

解密运算为：

$m_i=D(c_i) = c_i^d \bmod(n)$

在以上两式中，$m_i$为将编码明文M分组后所得之第i组明文，$c_i$为与之相对应的第i组密文。E、D分别表示加密和解密算。

在PK卡内基于上述原理利用软件实现该加解密算法。

本发明的具体实施电路图如图 3 所示。参见图 3，其中，D1 为 ST7261 芯片，U1 为双界面 PK 卡，J2 为 USB 接口，微型射频天线直接与双界面 PK 卡相连，由 C1、C2 和 T1 组成震荡电路，由三极管及其偏置电阻构成电源控制电路，由发光二极管 H1 和电阻 R2 构成指示灯电路。本发明通过所述的双界面 PK 卡，实现支持 1024 位非对称密钥算法，支持卡内密钥生成、加密、解密、签名、验证，同时支持 3DES 以及国密办指定的国产加密算法 SSF33。同时，本发明不仅具有 USB 接口，还具有射频接口，因此通过射频天线，可以在非接触状态下直接与外部射频读写器进行通讯，使用方便快捷。并且本发明内附符合 CSP、PKCS#11 规范的软件接口，能实现加密解密、证书管理和高度安全的 SSL 通讯功能，故能为用户端提供在 Internet 和 Intranet 上的安全通信，实现与浏览器的无缝连接，并且支持访问安全网站、加密邮件传送和对表单进行签字等功能。

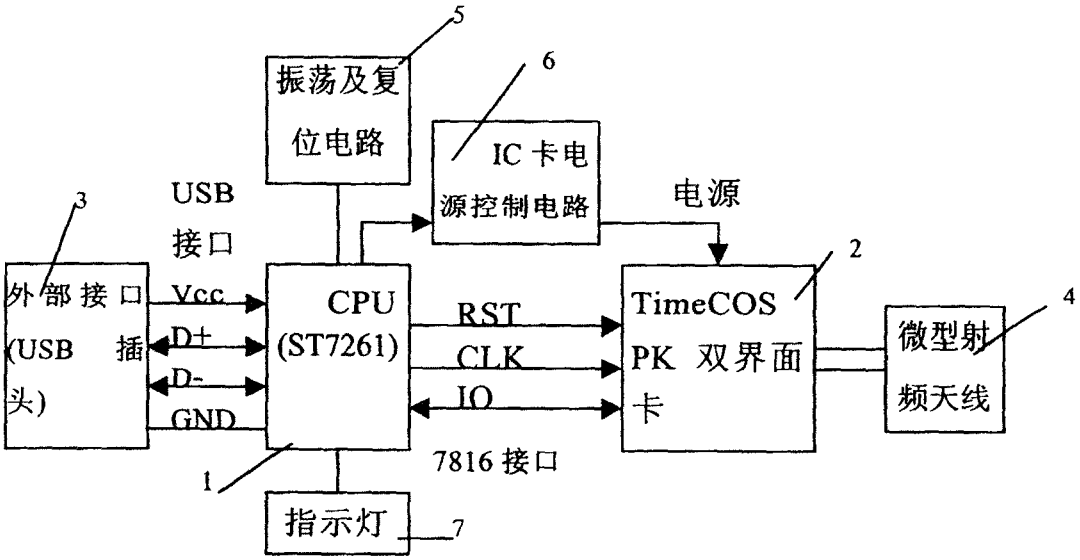

5
振荡及复位电路
6
IC卡电源控制电路
电源
3
USB接口
外部接口(USB插头)
Vcc
D+
D-
GND
CPU (ST7261)
RST
CLK
IO
7816接口
TimeCOS PK双界面卡
2
微型射频天线
4
1
指示灯
7

图 1

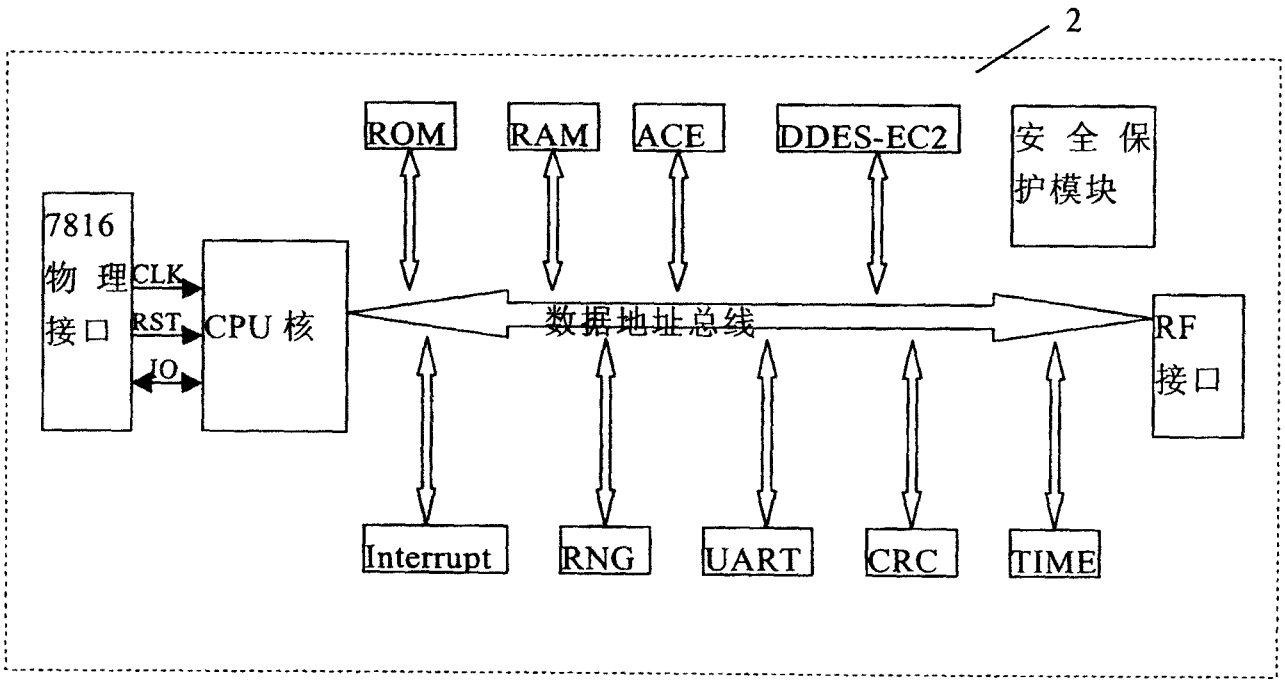

2
ROM
RAM
ACE
DDES-EC2
安全保护模块
7816物理接口
CLK
RST
IO
CPU核
数据地址总线
RF接口
Interrupt
RNG
UAART
CRC
TIME

图 2

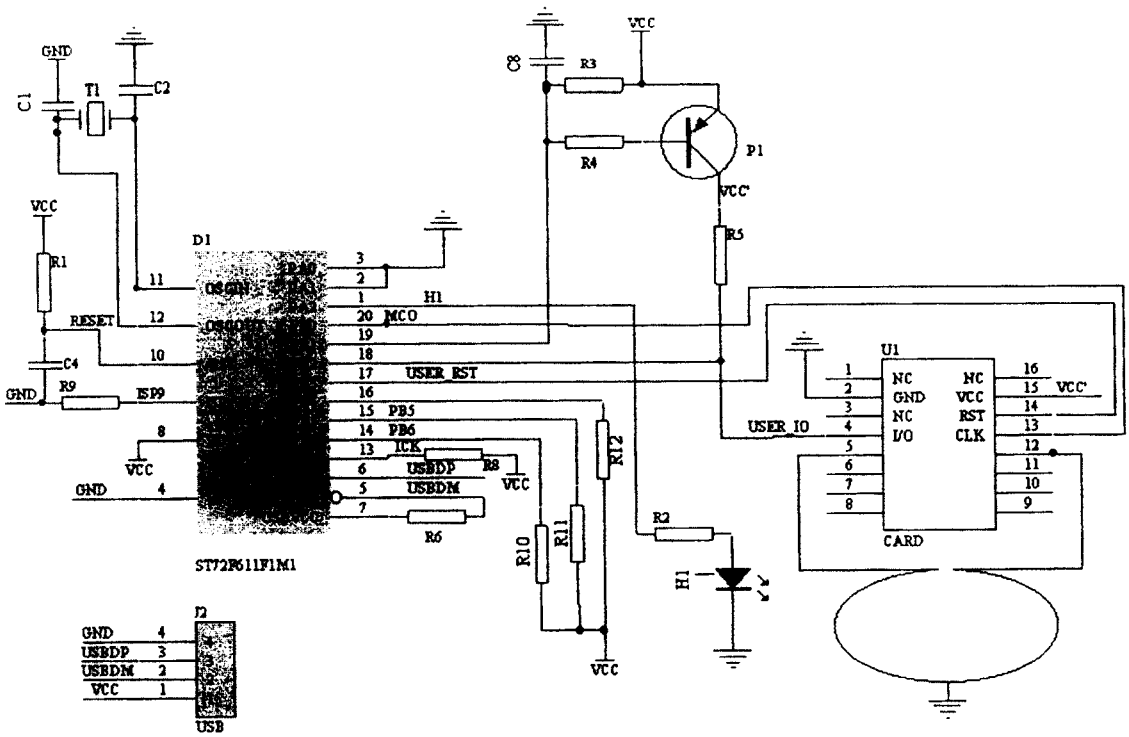

GND
C1
T1
C2
VCC
R1
RESET
C4
GND
R9
ISP9
VCC
GND
D1
11
12
10
8
4
3
2
1
20
19
18
17
16
15
14
13
6
5
7
MCO
H1
USER_RST
PB5
PB6
ICK
USBDP
USBDM
R8
R6
ST72F611F1M1
J2
GND 4
USBDP 3
USBDM 2
VCC 1
USB
C8
R3
R4
P1
VCC'
R5
R12
R10
R11
VCC
R2
H1
U1
NC
GND
NC
I/O
NC
VCC
RST
CLK
CARD
USER_IO
VCC'

图 3