



[12] 发明专利申请公开说明书

[21] 申请号 03147555.8

[43] 公开日 2005 年 1 月 26 日

[11] 公开号 CN 1570954A

[22] 申请日 2003.7.22 [21] 申请号 03147555.8

[71] 申请人 中国科学院自动化研究所
地址 100080 北京市海淀区中关村南一条 1 号

[72] 发明人 田捷 张堂辉 刘旭

[74] 专利代理机构 中科专利商标代理有限责任公司

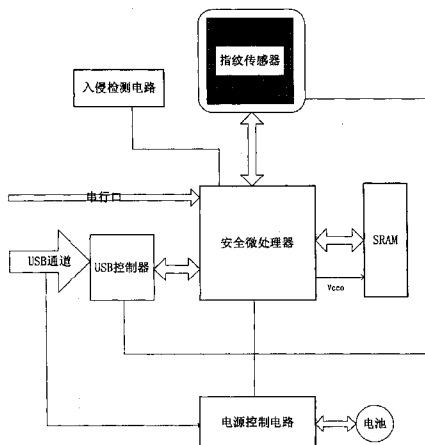
代理人 戎志敏

权利要求书 1 页 说明书 6 页 附图 2 页

[54] 发明名称 基于指纹的数字证书保护装置

[57] 摘要

一种基于指纹的数字证书保护装置，包括：非易失性 SRAM，用于存储数字证书和指纹认证算法及通信程序；安全微处理器，用于执行有的关程序；电源管理电路，用于管理系统的电源；入侵检测电路，用于防止黑客入侵；指纹传感器，用于注册指纹信息；通用串行总线控制器，用于主机和微处理器之间的通信。本发明使用指纹识别技术来验证合法用户，取代了传统的口令保护方法，因而避免了密码的失窃和密码记忆的问题。由于使用了指纹识别技术，所以大大方便了数字证书的使用。另外在装置中我们使用了安全微处理器和 SRAM 作为程序和数据的存储器，解决了数字证书的非法复制问题。该装置使用了软、硬件加密相结合的方法，可以保证数字证书的极高安全性。



1. 一种基于指纹的数字证书保护装置，其特征在于包括：
 - 5 非易失性 SRAM，用于存储数字证书和指纹认证算法及通信程序；
 - 安全微处理器，用于执行有关程序；
 - 电源管理电路，用于管理系统的电源；
 - 入侵检测电路，用于防止黑客入侵；
 - 指纹传感器，用于注册指纹信息；
 - 10 通用串行总线控制器，用于主机和微处理器之间的通信。
2. 按照权利要求 1 所述的数字证书保护装置，其特征在于：

所述的安全微处理器支持程序和数据总线的双 DES 加密，内部有密钥生成器，自举的时候具有密钥销毁功能。
3. 按照权利要求 1 所述的数字证书保护装置，其特征在于：
 - 15 所述指纹传感器采用 CMOS 半导体传感器，通过 8 位并行 IO 口和微处理器相连。
4. 按照权利要求 1 所述的数字证书保护装置，其特征在于：

所述的电源管理电路包括智能充电管理芯片、电源切换芯片和直流电压变换芯片。
- 20 5. 按照权利要求 1 所述的数字证书保护装置，其特征在于：

所述的入侵检测电路包括接地开关。

基于指纹的数字证书保护装置

5

技术领域

本发明涉及指纹识别技术，特别涉及基于指纹的数字证书保护方法及装置。

10 背景技术

随着计算机技术和网络技术的发展，全球经济发展正在进入信息经济时代。电子商务的诞生和发展，给世界经济带来巨大的变革和深远的影响。但是电子商务面临的最重要的问题就是如何保证因特网上信息传输的安全。目前普遍采用 PKI 技术(公钥基础设施)来保护信息的安全。PKI

15 技术采用证书管理公钥，通过第三方的可信任机构——认证中心 CA，把用户的公钥和用户的其他标识信息捆绑在一起，在因特网上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

20

数字证书是进行网上信息交流及商务活动的身份证明，在电子交易的各个环节，交易的各方都需验证对方证书的有效性，从而解决相互间的信任问题。通常数字证书是存放在使用者计算机的硬盘或者软盘上的，比如普通人使用的网上银行证书。对于安全性要求更高的企业用户，证书存放在专用的 IC 卡上。一种安全的数字证书保护方法，至少应该满足

25 两个条件：第一条，该数字证书只能被合法的用户所使用；第二条，被保护的数字证书除了证书发放机构外，应该是无法被复制的。对于第一条，传统的存放在各种介质上的证书，一般都使用口令进行加密。使用者在使用证书的时候，会要求用户输入证书密码来验证合法的用户。但是这种方法存在密码容易被窃取和密码的记忆问题。由于密码失窃，导致

30 银行储户的钱被非法用户提取的案例已经是屡见不鲜了。而这些案例

都是用户的密码被偷看或者使用者使用了诸如生日，门牌号等容易被猜测的密码导致。理论上如果密码的长度足够长，并且设定合理，用口令保护的安全性是能够保证的。但是同时带来的记忆负担往往是难以承受的，而且使用的时候很不方便。对于第一条，我们的装置中使用指纹识别技术来解决，我们将会在后面详细叙述。对于第二条，显然存储在硬盘和软盘上的证书是很容易被复制的，即使是有些存到 IC 卡内的证书，虽然也经过加密，但是对于有经验的人来说，复制起来也是有可能的。有些高档的带 CPU 的 IC 卡是可以保证在现有的技术下是不可复制的，但是仍然无法解决第一个问题。而我们的装置将使用特殊的加密方法和通信机制，来保证数字证书的不可复制。

二十世纪九十年代，作为一种比较成熟的生物特征识别方法，指纹识别技术开始得到广泛的应用。由于自动指纹识别系统价格的大幅度下降，自动指纹识别的应用不再仅局限于法律、公安领域。它可作为计算机确认用户的手段，可作为访问网络资源的信息安全技术，还可用于银行 ATM 卡和信用卡使用的确认、各类智能 IC 卡的双重确认、雇员证明和家用电子门锁等许多方面。

由于指纹具有唯一性和稳定性的优点，而且采集方便，成本低廉，所以非常适合取代传统的口令进行证书加密。本发明就是为了解决数字证书的安全问题，利用指纹技术来保护证书的一种装置。

20

发明内容

本发明的目的是提供一种实用的数字证书保护装置。

为实现上述目的，基于指纹的数字证书保护装置，其特征在于包括：

非易失性 SRAM，用于存储数字证书和指纹认证算法及通信程序；

25

安全微处理器，用于执行有关程序；

电源管理电路，用于管理系统的电源；

入侵检测电路，用于防止黑客入侵；

指纹传感器，用于注册指纹信息；

通用串行总线控制器，用于主机和微处理器之间的通信。

30

本发明使用指纹识别技术来验证合法用户，取代了传统的口令保护

方法，因而避免了密码的失窃和密码记忆的问题。由于使用了指纹识别技术，所以大大方便了数字证书的使用。另外在装置中我们使用了安全微处理器和 SRAM 作为程序和数据的存储器，解决了数字证书的非法复制问题。该装置使用了软硬件加密相结合的方法，可以保证在现有科学技术下，数字证书保护的极高安全性。

附图说明

图 1 是数字证书保护装置的构成框图；

图 2 是电路原理图。

10

具体实施方式

我们的目的是要实现一种安全的数字证书保护方法和装置。该装置应该是不可复制的，而且使用指纹识别技术代替口令来实现身份认证。为了保证数字证书的安全，该装置还应该能够抵抗黑客的软件和硬件攻击。

15

本发明装置的组成如图 1 所示，包括非易失性 CMOS SRAM，安全微处理器，电源管理电路，通用串行总线（USB）控制器，指纹传感器，入侵检测电路，串行数据口。

20

本发明采用非易失性 CMOS SRAM 来保存数字证书和指纹认证算法以及通信等其他程序。大多数 IC 卡采用的是电可擦写的闪存来存放数据，它们内部保存的数据在电源被清除后，数据可以保持上百年。这是一个最危险的安全缺陷，它给黑客无限长时间来突破芯片内的物理防线，可能导致数据的泄密。我们使用的这种 SRAM 里的数据只需要极小的电流就可以保证不会丢失，使用备份体积很小的锂电池，可以保证在没有外部电源的情况下，保持 SRAM 里的数据 10 年以上。但是 SRAM 响应速度非常快，在系统检测到入侵行为的时候，可以迅速被擦除或“清零”。

25

本发明采用的是安全微处理器来执行有关程序。这种处理器在内部自举程序控制下，利用双密钥三 DES 加密算法和外部进行通信。程序和数据总线上都有专门的加密和解密引擎。这样就可以防止黑客通过逻辑分析仪对总线上的数据进行监视，而这往往是使用 SRAM 系统的最大缺

30

陷。这样在 SRAM 存储器中程序、数据、算法等都是加密过的，保证了这些内容不可被复制。因为即使这些数据被黑客复制，由于无法获得加密密钥，这些内容也是不可读的。对加密操作起决定作用的加密密钥，是在处理器内部的，在微处理器自举的时候就已经确定。作为侵入响应的一部分，一旦发现侵入现象，这些密钥会被瞬间擦除，同时外部 SRAM 的所有内容也将瞬间被擦除。

本发明所述的电源管理电路如图 2 所示，主要由一个智能充电管理芯片 U7，电源切换芯片 U5，直流电压变换芯片 U6 组成。U6 芯片 Vout 连接微处理器和电池充电电路，而指纹传感器 U4 和 USB 接口芯片 U3 经过一个开关 MOS 管和 Vout 相连，电源切换芯片的状态线/VDDC 连接开关管的栅极，外接 SRAM 通过微处理器的 Vcco 供电。这样在 USB 通道打开的时候，由 USB 通道对整个装置供电，电源经过 U7 芯片为备份锂电池充电，并且可以看到充电指示灯亮。在 USB 通道关闭的时候，电源切换芯片将电源切换到备份锂电池。这个时候开关管切断了指纹传感器和 USB 控制器的电源，备份电池只向微处理器供电和 SRAM 供电。此外电源切换芯片状态线/VDCC 接到微处理器的中断引脚，微处理器检测到中断后，微处理器进入低功耗的深度休眠状态。

本发明的入侵检测电路原理如图 2，当装置的外壳被打开的时候，微处理器的自毁输入端的接地线被阻断，导致自毁输入端输入电平升高，这样微处理器将清除内部的密钥，内部 SRAM 数据被清除，同时微处理器会切断输出到外部 SRAM 的数据保持电压 Vcco，这样外部 SRAM 数据也被清除。

所述的指纹传感器是基于 CMOS 技术的指纹采集芯片，芯片的类型可以是平面型的，也可以条状扫描型的。这些传感器的特点是体积小，适合使用在各种嵌入式系统中。指纹传感器 U4 采集到的图像通过 8 位的并行 IO 数据线进入微处理器 U1，并且存储在 SRAM 芯片 U2 中。

所述的通用串行总线控制器 U3 能够使主机和微处理器 U1 之间通过 USB 接口进行传输数据，微处理器通过 8 位的并行 IO 数据接口和 USB 控制器相连。从主机来的数据流经过 USB 控制器，由 USB 控制器转发到微处理器。类似的，微处理器发送的数据流经过 8 位并行 IO 口，再由 USB

控制器转发到主机。

下面介绍该装置采用的通信方法，这个过程可以分为两部分：

1. 数字证书的下载

5 这个过程一般是在证书申请的时候完成的，这个证书的下载过程由证书发放机构完成。在申请的过程中，申请者需要注册自己的指纹模板信息。证书发放机构将以下数据通过装置的串行口写入 SRAM 中。

➤ 申请的数字证书

➤ 申请者的指纹模板数据

10 ➤ 本装置运行需要的程序和数据

为了保证数字证书的安全下载，下载过程分成两部分。首先是安全微处理器在内部自举程序控制下，从串口下载一个加密通信传输程序，然后使用这个加密通信传输程序下载数字证书、指纹模板以及其他程序和数据。已经下载过数字证书的装置，除非经过复位操作，不能重新下载证书。复位操作通过一个复位开关来实现，复位后安全微处理器重新自举，SRAM 中的数据被清除，本发明装置将回到初始状态。

15

2. 数字证书的使用

20 数字证书使用的时候 USB 接口进行数据传输，在使用前需要安装本发明装置的驱动程序。当网络应用程序需要使用数字证书进行数字加密或数字签名的时候，数字证书的读取步骤如下：

A. 首先通过主机的驱动程序向本发明装置发送开启命令；

B. 本装置收到开启命令后，发送应答消息，并且发送等待输入指纹的消息；

25

C. 用户在本装置的指纹传感器上按下手指，采集指纹数据。如果长时间不按手指，则退回到原始状态，并且发送一个装置关闭的消息给主机；

D. 本装置的处理使用 SRAM 力存储的指纹算法对指纹数据进行处理，得到指纹特征信息，并且将该特征信息和原来注册的指纹特征信息进行匹配。匹配成功则继续，匹配失败则回到步骤 B；

30

-
- E. 本装置向主机发送设备已开启消息，主机收到设备开启消息则发送读取数字证书的命令；
 - F. 收到读取数字证书的命令后，将数字证书内容发送给主机；
 - G. 主机收到数字证书后，发送关闭命令；
- 5 H. 本装置退回到原始状态，并且发送一个装置关闭的消息给主机。
- 数字证书的使用过程中，信息的传送将使用常见的加密传输方法，这个加密解密过程由驱动程序来实现，对应用系统是透明的。

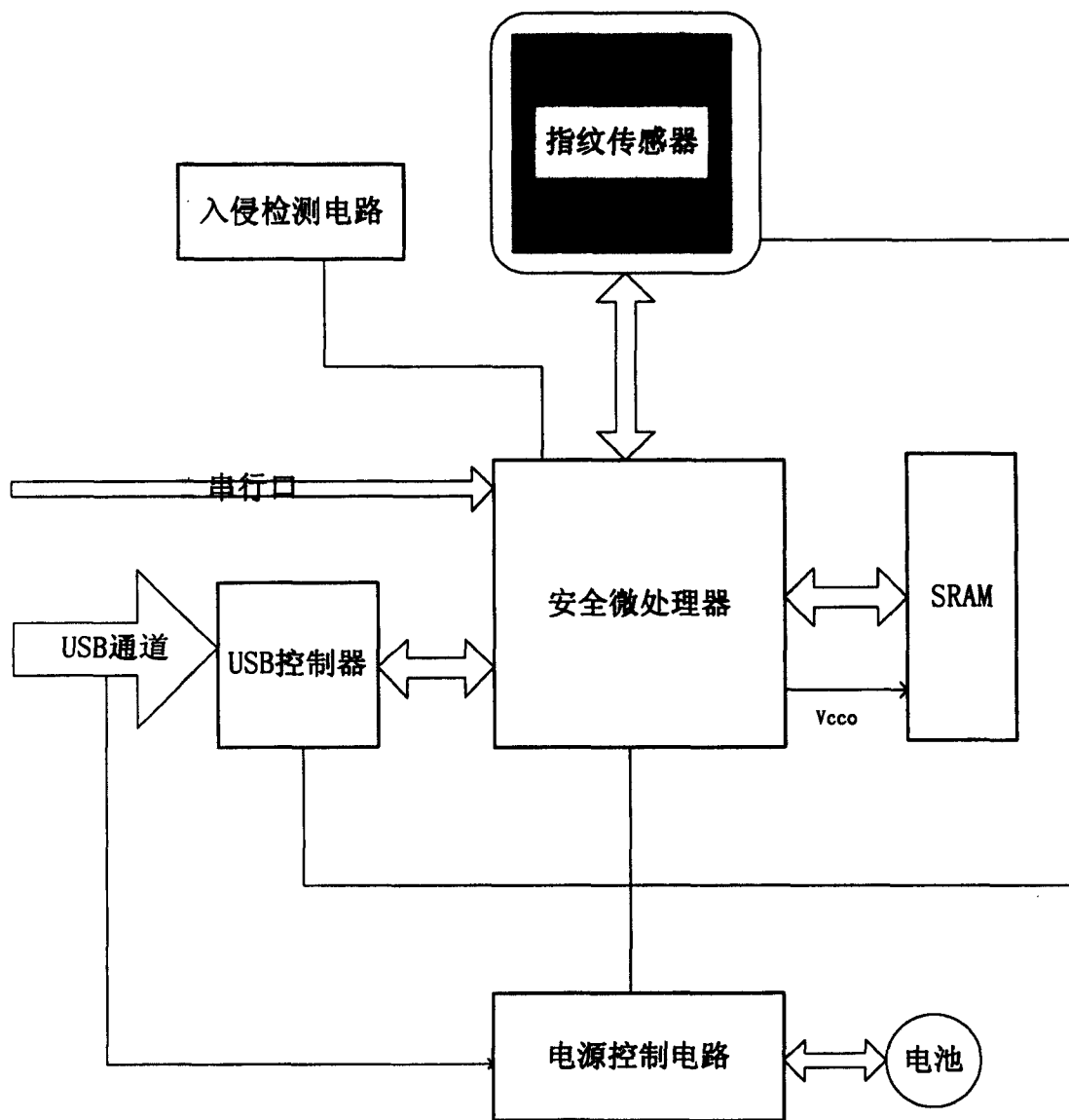


图 1

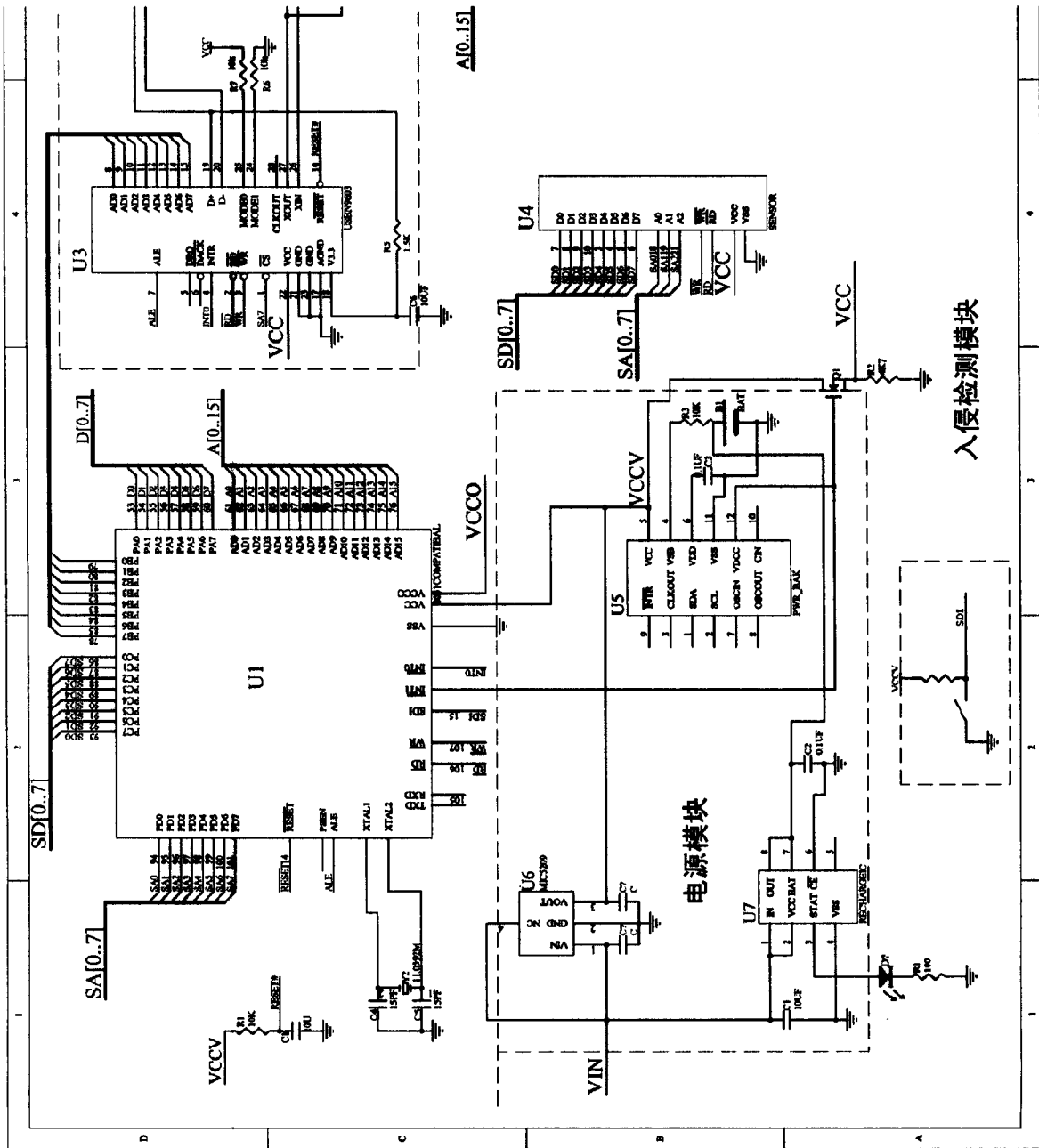


图 2