[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06F 13/38 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610169855.2

[45] 授权公告日 2008 年 11 月 26 日

[11] 授权公告号 CN 100437618C

[22] 申请日 2006.12.29
[21] 申请号 200610169855.2
[73] 专利权人 北京飞天诚信科技有限公司
地址 100083 北京市海淀区学院路 40 号研 7 楼 5 层
[72] 发明人 陆 舟 于华章
[56] 参考文献
CN2762204Y 2006.3.1
WO2006/119637A1 2006.11.16
US2002/0010827A1 2002.1.24
CN1317744A 2001.10.17
CN1885298A 2006.12.27
External Serial ATA WHITE PAPER. 第 4 页 6.21 行、图 2.4,Silicon Image,Inc.. 2004
审查员 欧阳琦

[74] 专利代理机构 北京三高永信知识产权代理有限责任公司
代理人 何文彬

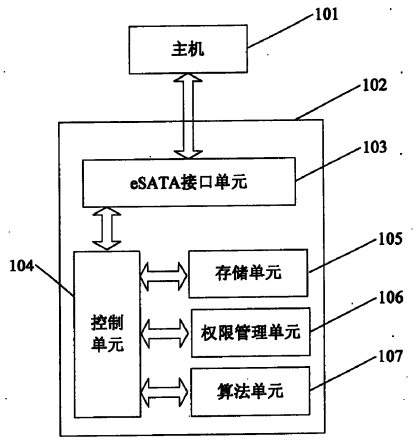
权利要求书 2 页 说明书 10 页 附图 2 页

[54] 发明名称

一种便携式信息安全设备

[57] 摘要

本发明公开了一种便携式信息安全设备，属于信息安全领域。为了解决 USB Key 数据传输速度低，和在 USB 主/从传输协议下，会占用较多 CPU 资源的问题，同时也为了满足下一代接口技术的发展，本发明提供了一种基于串行 ATA 协议的便携式信息安全设备，便携式信息安全设备包括 eSATA 接口单元、存储单元、权限管理单元、算法单元和控制单元。



1.一种便携式信息安全设备,其特征在于，所述信息安全设备包括 eSATA 接口单元、存储单元、权限管理单元、算法单元和控制单元；

所述 eSATA 接口单元用于将信息安全设备与主机通过 eSATA 接口建立连接，并按照外接串行 ATA 协议与所述主机进行通信，提供数据发送到 eSATA 定义总线和从 eSATA 定义总线接收数据的接口；

所述存储单元用于存储所述信息安全设备的内部数据；

所述权限管理单元用于根据访问所述信息安全设备的用户身份信息对其访问权限进行管理和控制；

所述算法单元用于进行加/解密运算；

所述控制单元用于控制所述 eSATA 接口单元与所述主机间的通信，控制所述权限管理单元对信息安全设备的访问操作，以及对所述存储单元中存储的数据进行控制和处理；

所述主机通过所述 eSATA 接口单元为所述信息安全设备供电；

所述主机按照外接串行 ATA 协议通过 eSATA 接口单元识别所述信息安全设备，并为所述信息安全设备分配地址以及根据所述信息安全设备的需求分配盘符；

所述主机发出操作指令到所述信息安全设备的 eSATA 接口单元，请求信息安全设备服务；

所述信息安全设备通过所述 eSATA 接口单元接收所述主机发来的操作指令，并通过所述 eSATA 接口单元向所述主机返回指令执行结果或信息。

2．如权利要求 1 所述的便携式信息安全设备，其特征在于，所述存储单元还用于存储密钥数据，所述密钥数据包括数字证书、密钥和用户私有数据。

3．如权利要求 1 所述的便携式信息安全设备,其特征在于，所述存储单元还用于存储用户程序，所述用户程序用来实现用户自定义算法的写入和调用。

4．如权利要求 2 所述的便携式信息安全设备，其特征在于，所述算法单元根据所述密钥数据进行加/解密运算。

5.如权利要求 1-4 中任意一项权利要求所述的便携式信息安全设备,其特征在于，所述控制单元为安全设计芯片，所述安全设计芯片包括智能卡芯片。

6.如权利要求 1-4 中任意一项权利要求所述的便携式信息安全设备,其特征在于，所述控制单元与所述存储单元、所述权限管理单元、所述算法单元和所述 eSATA 接口单元中的一个或几个集成在一颗芯片中。

7．如权利要求 6 所述的便携式信息安全设备,其特征在于，所述芯片为安全设计芯片，所述安全设计芯片包括智能卡芯片。

8.如权利要求 1-4 中任意一项权利要求所述的便携式信息安全设备,其特征在于，所述 eSATA 接口单元为分立的 eSATA 协议转换芯片。

一种便携式信息安全设备

技术领域

本发明涉及信息安全领域，特别涉及一种便携式信息安全设备。

背景技术

近几年，随着互联网技术与电子商务的快速发展，越来越多的商务活动转移到网络上开展，例如网上政府办公、网上数字银行、网上购物等等，与此同时，越来越多涉及个人隐私和商业秘密的信息需要通过网络传递。然而病毒、黑客、网络交易以及网页仿冒诈骗等恶意威胁，给在线交易的安全性带来了极大的挑战。

信息安全设备是一种带有处理器和存储器的小型硬件装置，它通过计算机的数据通讯接口与计算机连接。它具有密钥生成、安全存储密钥、预置加密算法等功能。信息安全设备与密钥相关的运算完全在装置内部运行，且信息安全设备具有抗攻击的特性，安全性极高。信息安全设备一般通过 USB 接口与计算机相连，通常被称为 USB KEY 或 USB Token。信息安全设备生产商、软件系统开发商或者最终用户可以将一些重要信息存储到信息安全设备中，用以保证安全性或者防止遗忘。目前，较高端的信息安全设备是可编程的，即可以实现在信息安全设备中运行预先存入其中的代码。

一般信息安全设备中会内置安全设计芯片来实现信息安全功能。安全设计芯片除了具有通用嵌入式微控制器的各种特性外，更多的是在安全性能方面，安全设计芯片在芯片设计时会针对安全性能方面在结构上做一些特殊处理，比如安全芯片会采用特定的安全内核，该安全内核能够支持多个拥有不同权限定义的状态，用于实现对硬件资源访问权限的管理；以及支持指令执行时间（指令周期）的随机化；其中断系统能够实现支持芯片状态的转换，从而实现对不同层次的安全级别的控制，以支持多应用的实现；还可以带有 MMU 单元(memory management unit，存储器管理单元)，用于实现逻辑地址、物理地址的隔离，及地址映射，从体系结构上支持应用（多应用）、安全性的设计实现，与内核支持的不同状态一起有机的组成一个硬件防火墙；其中断系统还能支持系统数据库与用户程序的接口及权限传递和切换；其存储介质方面也会采用非易失性存储介质等等。安全设计芯片一般都要求符合相关的标准及通过相关的认证等以保证其安全性能，比如 TCG TPM v1.2 规范，ISO15408 国际标

准，中国密码管理委员会标准等等。目前市面上有很多款安全设计芯片可供选择，其中意法半导体的 ST19WP18 微控制器，已通过“公共标准”评估保障级 EAL5+(增强版)的认证，这是 ISO15408 国际标准关于此类产品的最高的标准之一。

一般信息安全设备中会内置安全设计芯片来实现信息安全功能。信息安全采用集成电路技术后，使得信息安全得到了更好的保护，被保护信息的安全度也因此而有所提高，基于此概念设计的专用于信息安全保护方面的芯片习惯上被称为安全设计芯片。安全设计芯片一般通过下列三种方式来实现被保护信息的处理：将信息处理算法完全用硬件实现（逻辑加密型），将信息处理算法完全用软件实现（智能型），将信息处理算法部分用硬件、部分用软件来实现（可编程逻辑加密型）。

当前在计算机系统里使用的最广泛的硬盘接口是集成磁盘电子接口，简称 IDE 接口(Integrated Drive Electronics)。IDE 接口，更准确的称呼是 ATA (Advanced Technology Attachment-高级技术配件) 接口，目前通用的是并行接口方式，也称并行 ATA(Parallel ATA)接口，该接口起始于 1986 年，在 1988 年形成标准，主要提供一种规范方法使磁盘附属到个人计算机，近些年来，为了满足处理单元对硬盘数据访问速度的提高，ATA 接口技术的不断发展，已形成多种标准规范，如 ATA/ATAPI，EIDE，ATA-2，高速 ATA，ATA-3，Ultra ATA，Ultra DMA，ATA/ATAPI-4，ATA/ATAPI-5，ATA/ATAPI-6 等。

并行 ATA 接口在当前台式计算机以及便携式计算机内部的硬盘之间连接占据统治地位，是因为它简单、低成本等因素，然而并行 ATA 接口有一系列的限制因素，使人疲惫于不断增加其性能。这些受限的因素包括：高针数，40 针 80 芯电缆，且电缆长度短，不方便硬盘的接入及系统的散热要求，以及并行 ATA 接口的其他特性使该接口的数据传输速率在过去不能得到较快的发展，以致于并行 ATA 接口正接近于它的性能容量，不能满足计算机对数据传输速度的进一步增加需求。

基于这些因素，为满足下一代接口技术发展的需求，串行 ATA 接口发展为下一代 ATA 规范。SATA（Serial Advanced Technology Attachmen-串行高级技术配件）接口技术，即 Serial ATA，是最近两年在存储领域新发展起来的技术。Serial ATA，采用“序列式”的结构，把若干比特位数据打包，然后采用比并行式更高的速度，以数据分组的形式传输至主机，进行数据传输。

SATA 接口具有如下的主要特征：

1．高速度：现行的并行 ATA 接口很少会达到数据线最大的带宽，即使是 ATA/133 硬盘，也不会真正达到 133MB/S 的速率，最多也就只能达到 60MB/S 的稳定传输速率，而串行 ATA 最

大将实现 600MB/S 的传输速率。

2.点对点通信方式：由于串行 ATA 采用点对点的传输协议，所以不存在主/从问题，这样每个驱动器不仅能独享带宽，而且使拓展 ATA 设备更加便利，用户不需要再为设置硬盘主从跳线而苦恼，只要增加通道数目，即可连接多台设备。

3．支持热插拔：SATA 支持热插拔，像 USB 和 IEEE1394 一样，在不关机的情况下就能完成增加或移除硬盘的工作，并且不会对硬盘和控制器造成损坏。

4．内置数据校验：SATA 在传输总线的两头都引入了全新的 CRC（循环冗余校验）保护系统，SATA 的双向 CRC 校验对一般家庭用户用处可能不大，但对于高端工作站和服务器来说却是至关重要的。

SATA 接口是并行 ATA 接口的发展，该技术相对并行 ATA 有一个低得多的针脚数，线缆更软，提供硬盘更长的接入线缆，方便硬盘接入主机系统，且支持热插拔，此外，SATA 接口采用较低针脚数也有益于主板包括芯片及其它集成的硅零部件在内的系统设计，便于外置和移动使用，能够满足下一代接口技术发展的需要。

在移动存储方面，eSATA（External Serial ATA-外接串行高级技术配件）技术也开始走入我们的视线，即将 SATA 端口由主板内引出到机箱外面来。eSATA 作为 SATA 接口的外部扩展规范，eSATA 的优势也是显而易见的，和常见的 USB2.0 和 IEEE1394 两种常见外置接口相比，eSATA 最大的优势就是数据传输能力，eSATAd 的传输速率可达到 300MB/s，远远高于 USB2.0 的 480Mbp/s 和 IEEE 1394 的 400Mbp/s，并且依然保持方便的热插拔功能，即用户是不需要关机便能随时接上或移除 SATA 装置，十分方便。随着 eSATA 的出现，外置接口的传输率也首次远远大于了硬盘等设备的内部传输率。目前，包括希捷等在内的多家存储厂商都开始把自己的业务重点转向外置式硬盘，在 CES2006 上，希捷就展示了最新研发的 eSATA 按键备份系列外置硬盘，其中 500GB 容量产品的接口速度高达 300MB/s；此外，Data-Tec、I-O DATA 等公司也纷纷推出了各自的 eSATA 外置硬盘或 DVD 刻录机，与此同时，市场上也出现了带有 eSATA 接口的主板产品，如华擎的 775XFire-eSATA2、ASUS 的 P5W DH 等，另外 Seagate 公司也设计生产了 eSATA 外置硬盘等产品。

目前广泛使用的 USB Key 存在如下不足之处：

1.由于目前 USB 的最大传输速度只能达到 10MB/S，大大地限制了数据传输的速度。

2.USB 技术是基于主/从式传输协议，相对点对点的传输协议而言，会占用较多 CPU 资源。

发明内容

为了解决USB Key数据传输速度低，以及USB主/从传输协议会占用较多CPU资源的问题，同时也为满足下一代接口技术的发展需要，本发明提供了一种基于外接串行ATA协议的便携式信息安全设备，具体说是将目前广泛使用的信息安全设备采用外接串行ATA技术实现。所述信息安全设备包括eSATA接口单元、存储单元、权限管理单元、算法单元和控制单元；

所述eSATA接口单元用于将信息安全设备与主机通过eSATA接口建立连接，并按照外接串行ATA协议与主机进行通信，提供数据发送到eSATA定义总线和从eSATA定义总线接收数据的接口；

所述存储单元用于存储所述信息安全设备的内部数据；

所述权限管理单元用于根据访问信息安全设备的用户身份信息对其访问权限进行管理和控制；

所述算法单元用于进行加/解密运算；

所述控制单元用于控制所述eSATA接口单元与主机间的通信，控制所述权限管理单元对信息安全设备的访问操作，以及对所述存储单元中存储的数据进行控制和处理。

所述存储单元还用于存储密钥数据，所述密钥数据包括数字证书、密钥和用户私有数据。

所述存储单元还用于存储用户程序，所述用户程序用来实现用户自定义算法的写入和调用。

所述算法单元根据所述密钥数据进行加/解密运算。

所述控制单元为安全设计芯片，所述安全设计芯片包括智能卡芯片。

所述控制单元与存储单元、权限管理单元、算法单元和eSATA接口单元中的一个或几个集成在一颗芯片中。

所述芯片为安全设计芯片，所述安全设计芯片包括智能卡芯片。

所述eSATA接口单元为分立的eSATA协议转换芯片。

有益效果：

1.由于信息安全设备与主机按照eSATA协议进行通信，而eSATA标准的传输速率可达到300MB/s,大大地提高了数据的传输速度。

2.由于eSATA使用的是点对点的传输协议，所以不存在主/从问题，节约了系统资源。

3.由于eSATA支持热插拔，所以信息安全设备与计算机的断开和连接都无需考虑计算机的运行状态，使用非常方便，同时也符合下一代接口技术的发展需求。

附图说明

图 1 是本发明实施例提供的便携式信息安全设备的结构图；

图 2 是本发明实施例提供的信息安全设备的控制方法流程图。

具体实施方式

下面结合附图和具体实施例对本发明作进一步说明，但不作为对本发明的限定。

实施例 1

如图 1 所示，本发明实施例提供了一种基于 eSATA 协议的信息安全设备 102，它包括 eSATA 接口单元 103、控制单元 104、存储单元 105、权限管理单元 106 和算法单元 107。控制单元 104 分别与 eSATA 接口单元 103、存储单元 105、权限管理单元 106 和算法单元 107 相连。基于 eSATA 协议的信息安全设备 102 通过 eSATA 协议与主机 101 进行通信。

控制单元 104 用于对数据信息进行控制和处理。控制单元 104 内置有安全模块，安全模块用于提供信息安全保护，控制单元可以为安全设计芯片，例如智能卡芯片。控制单元 104 通过 eSATA 接口单元 103 与主机 101 进行通信，并依据权限管理单元 106 管理和控制对信息安全设备 102 的访问操作，以及对存储单元 105 中存储的数据进行控制和处理。

eSATA 接口单元 103 用于与主机 101 建立连接，并按照 eSATA 协议进行通信，提供信息安全设备 102 数据输入/输出的端口，将数据发送到 eSATA 定义的总线和从 eSATA 定义的总线接收数据。eSATA 接口单元 103 支持遵从 eSATA 标准的 eSATA 功能，并在 eSATA 总线上进行设备的标识、列举、配置和登记信息安全设备 102 所需的 eSATA 接口功能。

存储单元 105 用于存储内部数据；还包括存储密钥数据，密钥数据具体包括数字证书、密钥和用户私有数据等；还可以用于存储用户程序，用户程序是用来实现用户自定义算法的写入和调用的，比如用来存储预置的加/解密算法，或者用户自定义的算法，或者存储部分用户代码等等。

权限管理单元 106 用于依据访问信息安全设备的用户身份信息对其访问权限进行管理与控制。

算法单元 107 用于实现加/解密处理；

存储单元 105 的存储介质可为 RAM、ROM、EPROM、EEPROM、FLASH 中的一个或几个组成。

由于 eSATA 接口标准支持热插拔的功能，如同 USB 和 IEEE1394 一样，在主机不关机的情况下就能完成添加或移除信息安全设备的动作，并且不会对信息安全设备 102 和其内的存储单元 105 造成损坏，为用户的移动使用提供了便利。

在实际的产品设计中，可以有多种实现形式，比如可以利用安全设计芯片实现控制模块的功能，利用存储芯片实现存储单元、权限管理单元和算法单元的功能，再利用一颗 eSATA 协议转换芯片实现 eSATA 接口单元的功能；也可以将控制单元与存储单元、权限管理单元、算法单元和 eSATA 接口单元中的一个或几个集成在一颗芯片（可以是安全设计芯片，包括智能卡芯片）中实现等。

本发明实施例的一个优选方案是采用带 eSATA 接口的智能卡芯片来实现对数据信息的总体控制和处理，可以实现信息安全设备与主机间的通信、对接收到的数据信息进行解析及处理，以及访问权限管理，另外，用来实现加/解密处理的算法等程序也存放在智能卡芯片中可修改的存储区中，以便于后期可以对其进行功能升级等操作。当用于身份认证等需要用到密钥数据的应用时，数字证书、公钥密钥或用户私钥等私有数据也会被存放在智能卡芯片的存储区中。

对于带有 eSATA 接口的智能卡芯片，其 eSATA 接口完全遵从 eSATA(External Serial ATA-外接串行高级技术配件）协议，用于将信息安全设备与主机建立连接，并按照 eSATA 协议与主机进行通信，提供数据发送到 eSATA 定义总线和从 eSATA 定义总线接收数据的接口。目前市面上能够提供符合 eSATA 协议的 eSATA 控制芯片有Silicon Image Inc. 的 Sil3531，能够提供一路符合 eSATA 协议的 eSATA 接口，支持最高传输速度达 300MB/s，另外，Silicon Image Inc. 还提供了支持 2 路符合 eSATA 协议的 eSATA 接口控制芯片，如 Sil3132、Sil3512 等。

将信息安全设备 102 通过智能卡芯片中提供的 eSATA 接口与主机相连后，主机便通过 eSATA 接口向信息安全设备进行供电，正常使用。这种采用带有 eSATA 的智能卡芯片实现信息安全设备的方案中，由于采用了整体封装，所以从整体上提升了系统性能。

在信息安全设备 102 与主机 101 相连接时，会产生一个标准的 SATA 列举过程，在这个过程中，主机 101 对信息安全设备 102 的配置模式进行配置。本发明实施例的信息安全设备 102 与主机 101 之间接口采用 eSATA 标准，按照 eSATA 接口协议的工作流程，与主机操作系统配合对信息安全设备进行初始化工作，由主机为信息安全设备 102 分配盘符，并按照主机操作系统的要求，进行接口标准操作，对信息安全设备 102 进行配置，然后，信息安全设备执行相应的操作指令，如数据交互操作，或身份认证信息处理操作，以及预置代码操作等。

上述优选方案的结构只是本发明的一个特例，在具体实施时，eSATA 接口单元 103 也可以设置在分立的 eSATA 协议转换芯片中，可应用的协议转换芯片种类比较多，比如 USB 协议转 eSATA 的桥接芯片有 Sunplus 公司的 SPIF216A 和 SPIF215A 等，另外还有 PATA 协议转 eSATA 协议的桥接芯片等。

主机 101 可以是台式电脑、笔记本电脑、服务器或专用机。本发明实施例实现的基于 eSATA 协议的信息安全设备也可以与其它外部设备进行连接，外部设备可以但不限于是读卡器、通讯设备、数码相机、计算机外设或其它专用设备。

实施例 2

参见图 2，是基于 eSATA 协议的信息安全设备的控制方法，包括以下具体步骤。

步骤 201：将信息安全设备通过 eSATA 接口与主机建立连接。

步骤 202：主机通过 SATA 接口向信息安全设备供电。

主机对应的 SATA 接口连接器检测到有设备接入，即向接入的信息安全设备供电。

步骤 203：信息安全设备获取设备描述符。

主机向信息安全设备发出问询指令，问询信息安全设备的描述符，信息安全设备根据问询指令，从其 eSATA 接口单元中获取设备描述符，该设备描述符含有标志，表明信息安全设备允许一个或多个盘符。信息安全设备将该设备描述符返回给主机。

步骤 204：主机为信息安全设备分配地址。

主机接收到该设备描述符后，为信息安全设备分配逻辑地址。

步骤 205：信息安全设备获得配置端点接口描述符。

主机再次发出问询指令，问询配置、端点和接口描述符，信息安全设备根据该问询指令获得上述描述符，并将该描述符返回给主机。描述符包含支持最大逻辑单元数的信息，即要求产生多少个盘符的标志。

步骤 206：检验描述符是否规范，如果不规范，则执行步骤 207，如果规范，则执行步骤 208。

步骤 207：禁止配置该设备，并进行再次问讯，执行步骤 203。

步骤 208：主机发命令准许设备配置。

主机向信息安全设备发出准许配置设备的质量，开始进行一系列信息安全设备配置操作。

步骤 209：主机发命令查询设备相关信息。

主机发出问询指令，问询设备相关信息，该信息包括设备厂商名、产品名等，启动相应设备驱动程序，选择接口、端点（管道），确定传输方式。

步骤 210：信息安全设备回答查询结果。

信息安全设备应答该问询指令，返回上述信息。

步骤 211：主机为信息安全设备分配盘符。

主机操作系统根据信息安全设备的要求，为信息安全设备分配一个或多个盘符。至此，主机对信息安全设备的识别、配置过程完毕。

步骤 212：将用户提供的认证信息与信息安全设备中存储的认证信息进行比对。如果比对结果一致，则执行步骤 213，否则提示错误，异常处理。

将用户提供的认证信息与信息安全设备中存储的用户认证信息进行比对，根据比对结果判断用户是否具有信息安全设备的访问权限。用户可以通过输入 PIN 码或生物特征信息的方式进行合法身份的验证。

步骤 213：主机发出对信息安全设备的操作指令。

主机发出操作指令到信息安全设备的 eSATA 接口，请求信息安全设备服务。

步骤 214：信息安全设备接收指令。

信息安全设备通过其 eSATA 接口接收主机的操作指令。

步骤 215：信息安全设备执行操作指令。

信息安全设备解释、执行该操作指令。

步骤 216：信息安全设备向主机返回指令执行结果或信息。

信息安全设备将操作指令执行结果、系统信息、操作数据等返回给主机。

步骤 217：主机检测用户是否移除信息安全设备，如果是，则执行步骤 318，否则重复执行操作指令的过程，直到用户移除、关闭信息安全设备。

步骤 218：主机停止向信息安全设备供电。

在接收到用户移除、关闭信息安全设备的信号后，主机和信息安全设备完成所有操作任务，停止供电，此时信息安全设备与主机断开连接。

当用户把信息安全设备从主机的 SATA 接口拔出时，主机操作系统自动检测到该设备已经从主机拔出，主机操作系统消除与信息安全设备对应的设备符。

在上述流程中，步骤 215 信息安全设备执行操作指令包括以下内容：

1. 数据交互操作

数据交互操作具体包括对写入的数据在信息安全设备内进行加密，或对读取的数据在信息安全设备内进行解密。数据加密和数据解密算法可以是 RSA、DES、3DES、SCB2、SSF33、AES、ECC 算法中的任意一种或任意几种。在对数据加密和解密时，程序存储单元中的固件程序会利用其中存储的算法，结合密钥数据存储单元中存储的密钥实现对数据的加密和解密操作。

2. 身份认证信息处理操作

身份认证信息处理主要包括存储/验证密码信息、存储/验证签名、存储/验证数字证书和权限管理。其主要应用在身份认证领域，利用密钥数据存储单元中存储的数字证书、密钥或用户私有数据进行安全的身份认证，主要可以实现如下功能：

a. 控制访问网络：通过识别信息安全设备中含有的硬件信息或密钥数据存储单元中存储的用户验证信息，来控制用户访问网络。

b. 用于验证和鉴别文件发送者身份的数字签名或证明，防止被中途篡改。

c. 存储密码信息：储存用户密码信息，防止用户手动输入密码时带来的风险。

d. 远程登陆：银行等网站可以利用签名信息来识别用户的合法性。

e. 控制文件的访问：可以在一些文件中加入访问控制信息，防止非法访问或运行信息安全设备。

f. 控制登陆到特定的应用系统：软件系统开发商可以将此功能用于自己的产品，即可以利用信息安全设备自动登陆特定的应用系统。

利用信息安全设备实现身份认证的主要作用是保护重要数据、敏感数据永远都不会被读出到装置之外，其好处是：

a. 用户可以不必记忆冗长的密码。安全的密码一定有字母和数字组成足够复杂的字符串，而且是时常更新的，而用信息安全设备来存储密码信息可以免去用户使用中的麻烦。

b. 提供双因子认证的保险措施，即使用户的密码或信息安全设备的丢失，都不会给用户带来风险。

c. 密钥存储在密钥数据存储单元中，不可导出，保证了安全性。

3. 预置代码操作

预置的代码，会被存储在程序存储单元中，实现了对软件产品的保护。预置代码包括预置用户软件部分片断，用户软件部分片断不能被读出信息安全设备，并使之在设备内部运行，与外部软件交互，依次来控制软件保证其合法运行。它可以实现如下软件保护功能：

a. 写文件：包括用户的代码片断，或者该片断运行时所需要的数据。

b. 读文件：包括代码片断运行时的数据文件，但不是该代码片断本身。

c. 运行文件：即用户写入的代码片断在信息安全设备内运行，并保证其运行的一切数据和相关信息保留在该设备内，而只返回结果。

预置代码还包括预置软件保护应用接口函数，软件保护应用接口函数是信息安全设备和软件系统开发商应用之间的接口函数，这个应用接口函数主要由软件系统开发商使用。它主要具备如下功能：

a.打开设备：打开信息安全设备，建立与其的通讯通道。

b.关闭设备：当主机不再使用该设备的时候，关闭该设备并清除设备状态信息。

c.送命令：实现对信息安全设备的所有设置工作，即所有软件保护功能的实现。

利用信息安全设备采用预置代码方式进行软件保护，关键是对于预置代码即保护程序的部分不会出现在主机的内存中，这样带来的好处是：

a.防止程序的非法拷贝：主机上的程序离开软件保护就是不完整的，即不能正常使用。

b.防止程序被非法跟踪或调试：使软件的关键代码不会在主机中运行，所有的调试软件都无法得到该段程序的运行状态。

c.防止被转储：软件最易被破解的途径是在运行的过程中，传统的加壳保护的软件，经常被内存转储而将代码还原回来。

d.防止反编译：无论反编译的技术有多高，都无法得到该预置代码片断。

在本控制方法中程序存储单元中存储的固件程序用来实现识别设备、等待并接收来自主机的数据、解析并处理数据、返回给主机数据、以及设备同主机断开连接。

以上所述的实施例只是本发明较优选的具体实施方式，本领域的技术人员在本发明技术方案范围内进行的通常变化和替换都应包含在本发明的保护范围内。

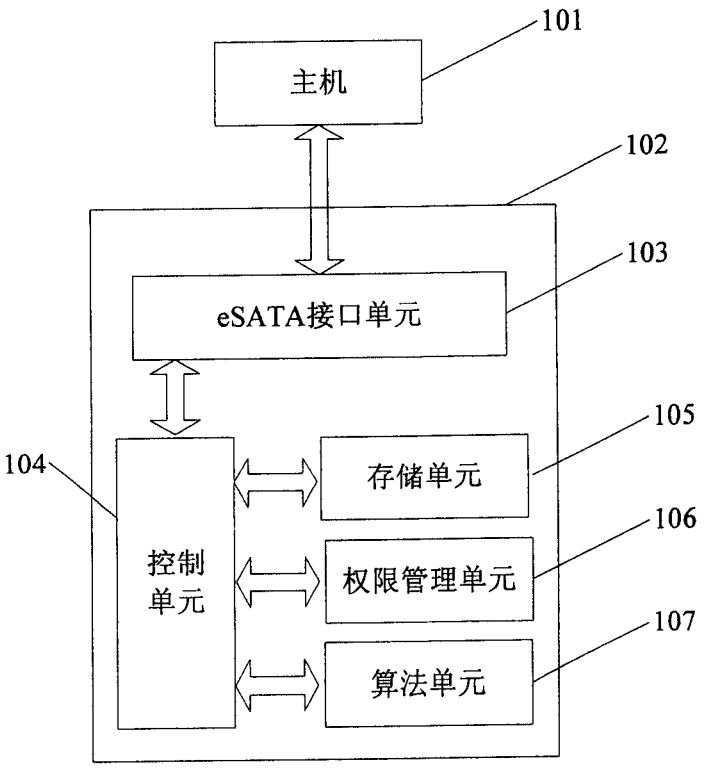

101
主机
102
103
eSATA接口单元
104
控制
单元
105
存储单元
106
权限管理单元
107
算法单元

图 1

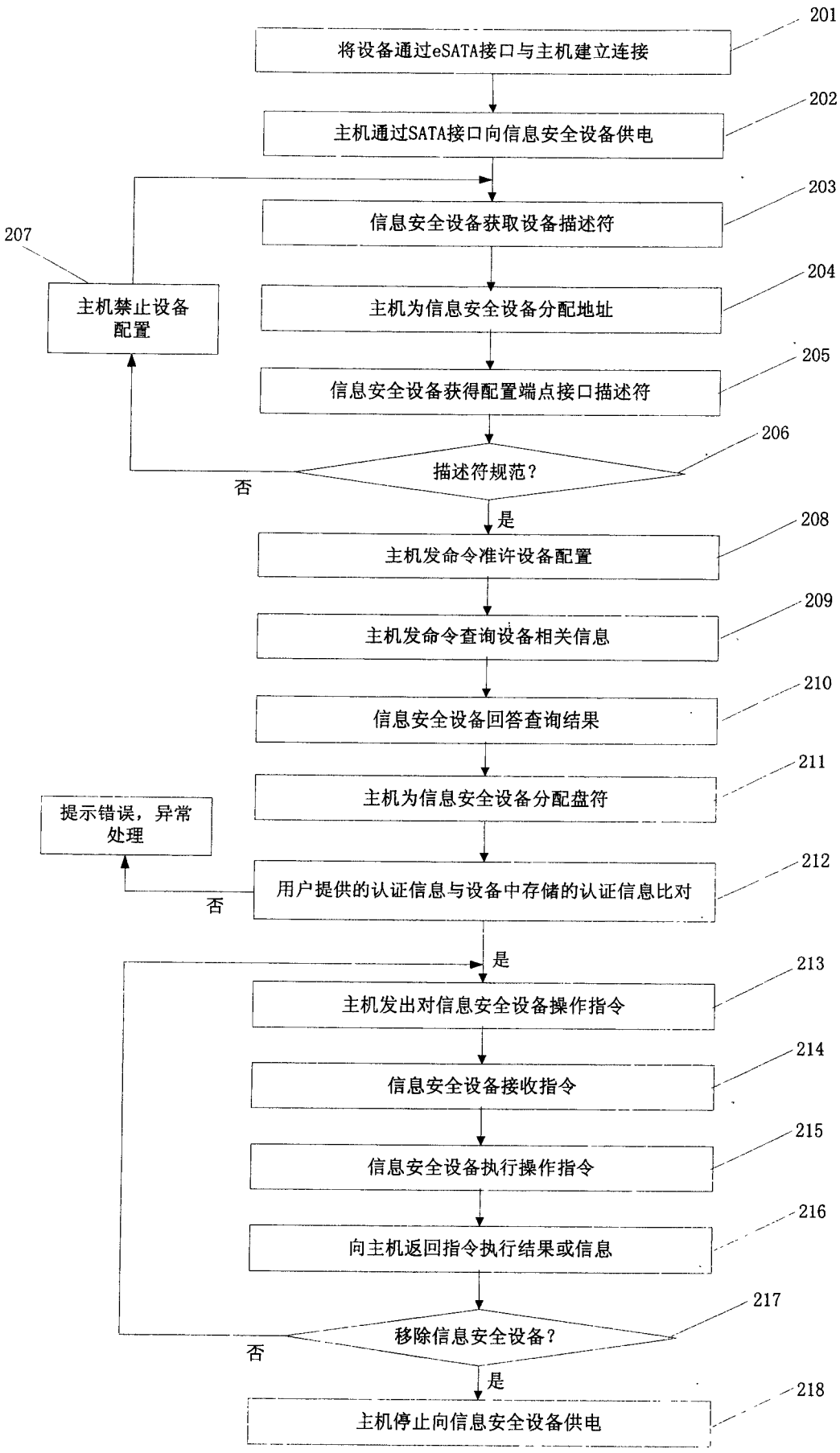

201
将设备通过eSATA接口与主机建立连接
202
主机通过SATA接口向信息安全设备供电
203
信息安全设备获取设备描述符
204
主机为信息安全设备分配地址
205
信息安全设备获得配置端点接口描述符
206
描述符规范？
否
207
主机禁止设备配置
是
208
主机发命令准许设备配置
209
主机发命令查询设备相关信息
210
信息安全设备回答查询结果
211
主机为信息安全设备分配盘符
212
用户提供的认证信息与设备中存储的认证信息比对
否
提示错误，异常处理
是
213
主机发出对信息安全设备操作指令
214
信息安全设备接收指令
215
信息安全设备执行操作指令
216
向主机返回指令执行结果或信息
217
移除信息安全设备？
否
是
218
主机停止向信息安全设备供电

图 2