[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510130655.1

[43] 公开日 2006 年 5 月 24 日

[11] 公开号 CN 1776563A

[22] 申请日 2005.12.19
[21] 申请号 200510130655.1
[71] 申请人 清华紫光股份有限公司
地址 100084 北京市海淀区清华园清华大学紫光大楼
[72] 发明人 菅晓翔 高 宏

[74] 专利代理机构 北京清亦华知识产权代理事务所
代理人 罗文群

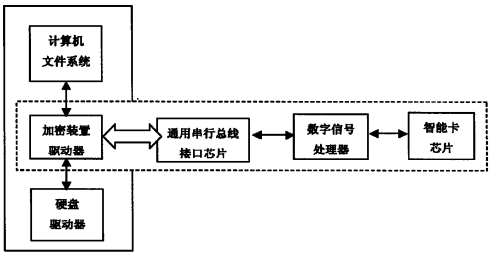
权利要求书 1 页 说明书 4 页 附图 1 页

[54] 发明名称

一种基于通用串行总线接口的文件夹加密装置

[57] 摘要

本发明涉及一种基于通用串行总线接口的文件夹加密装置，属于计算机信息安全技术领域。包括：通用串行总线接口芯片，与计算机主机相连接；数字信号处理器，与通用串行总线接口芯片相连接；智能卡芯片，与数字信号处理器相连接；加密装置驱动器，置于计算机内的文件系统驱动器与硬盘驱动器之间。本发明的计算机文件夹加密装置，整机和其中缩短密钥与计算机系统分离，可防止计算机丢失或被盗时产生的信息泄露危险。使用过程中对用户进行身份验证，可防止计算机硬盘中的信息泄露；可满足用户对不同安全等级的数据保护要求；利用智能卡芯片内的产品唯一序列号作为种子产生加密密钥，保证了加密密钥和加密装置的唯一性；使用安全、方便。



1、一种基于通用串行总线接口的计算机文件夹加密装置，其特征在于该装置包括：

（1）通用串行总线接口芯片，用于计算机主机与数字信号处理器之间的高速数据传输和通讯，与计算机主机相连接；

（2）数字信号处理器，用于对由计算机主机读取的数据流进行加密和解密，与通用串行总线接口芯片相连接；

（3）智能卡芯片，用于存储密钥和个人信息，与数字信号处理器相连接；

（4）加密装置驱动器，用于获取计算机主机中文件系统对计算机硬盘的读写操作，将多组16位的硬盘数据转换为一组128位的加密解密数据，控制加密装置对128位的数据进行加密解密，置于计算机内的文件系统驱动器与硬盘驱动器之间。

一种基于通用串行总线接口的文件夹加密装置

技术领域

本发明涉及一种基于通用串行总线接口的文件夹加密装置，属于计算机信息安全技术领域。

背景技术

计算机软、硬件系统的开放性、易用性和标准化等特点，使计算机存在先天性的致命安全隐患，导致计算机硬盘数据很容易被非法获取、盗用、篡改或破坏。

保证计算机数据安全的最有效办法是采用加密技术对数据进行加密，将原来的明文数据按某种算法进行处理，使其成为不可读的密文，保护关键数据不被非法用户窃取、阅读、篡改或破坏。

西北工业大学在申请号为200410025825.5的发明专利申请中，公开了一种“计算机硬盘数据加密方法及其装置”。该技术将数据加密装置放置在硬盘与主机之间，对计算机的硬盘和主机之间传输的数据进行加密。数据加密装置采用PCI总线，可直接插入计算机主板上的PCI插槽中。加密装置上有一IC卡读写口，可将合法用户持有的IC卡中的密钥，读取并存储到加密装置内的密钥管理模块中。

IBM公司在申请号为CN00131477.7的发明专利申请中，公开了一种“用不可访问的唯一密钥对储存的数据进行加密/解密”的方法及装置。该专利申请采用了对于该计算机系统而言是唯一的一个不可访问密钥。这个唯一密钥可以嵌入这一计算机系统的不可拆卸硬件中，或者可以从例如该计算机系统不可拆卸硬件的标识号产生。其中的处理过程包括构造这一唯一密钥，用这个密钥加密数据，并将加密数据存入存储媒介，而不需要将唯一密钥存入存储媒介。这一存储媒介可以包括任何不可拆卸或者可拆卸存储媒介，包括例如一个计算机硬盘、软盘或者可记录光盘。

上述两种方法均可防止硬盘丢失或被盗时，数据可被其它计算机读取的危险，但上述已有技术存在以下缺点：

1、西北工业大学的数据加密方法将加密/解密时使用的密钥存储在加密装置内的密钥管理模块中，IBM的数据加密方法中的密钥由计算机系统中不可拆卸硬件的标识号产生，如果整机丢失或被盗，这两种方法都不能保证硬盘内的数据安全。

2、对计算机硬盘中的全部数据进行加密，不能满足用户对不同安全等级数据的保护要求。

发明内容

本发明的目的是提出一种基于通用串行总线接口的计算机文件夹加密装置，以防止计算机整机丢失或被盗时出现的信息泄露危险，将存有密钥的加密装置与计算机系统分离，实现对计算机中信息的保护。

本发明提出的基于通用串行总线接口的计算机文件夹加密装置，包括：

（1）通用串行总线接口芯片，用于计算机主机与数字信号处理器之间的高速数据传输和通讯，与计算机主机相连接；

（2）数字信号处理器，用于对由计算机主机读取的数据流进行加密和解密，与通用串行总线接口芯片相连接；

（3）智能卡芯片，用于存储密钥和个人信息，与数字信号处理器相连接；

（4）加密装置驱动器，用于获取计算机主机中文件系统对计算机硬盘的读写操作，将多组16位的硬盘数据转换为一组128位的加密解密数据，控制加密装置对128位的数据进行加密解密，置于计算机内的文件系统驱动器与硬盘驱动器之间。

本发明提出的基于通用串行总线接口的计算机文件夹加密装置，具有以下优点：

1、本发明的加密装置及其中的密钥与计算机系统分离，可防止计算机整机丢失或被盗时产生的信息泄露危险。本加密装置对用户进行身份验证，因此即使加密装置和计算机一起丢失或被盗，也可防止计算机硬盘中的信息泄露。

2、本发明的加密装置设置在计算机内的文件系统与硬盘驱动器之间，可对指定的文件或文件夹进行加密，而不是对硬盘上的所有数据加密，满足用户对不同安全等级的数据保护要求。

3、本发明的加密装置中包括智能卡芯片，利用智能卡芯片内的产品唯一序列号作为种子产生加密密钥，即保证了加密密钥的唯一性，也保证了加密装置的唯一性。

4、双因素身份认证。只有在计算机通用串行总线接口插入本发明的加密装置，并输入正确的用户口令后，用户才能通过身份验证，对加密文件夹进行操作，因此身份认证的安全强度较高。

5、使用安全、方便。加密装置的形状和大小与闪存盘相当，用户可象使用钥匙一样，随身携带加密装置，可防止加密装置丢失或被盗。

附图说明

图1是本发明装置的结构框图，虚线框内为本发明装置，其它部分为计算机主机部分。

具体实施方式

本发明提出的基于通用串行总线接口的计算机文件夹加密装置，其结构框图如图1所示，包括：通用串行总线接口芯片，用于计算机主机与数字信号处理器之间的高速数据传输和通讯，与计算机主机相连接；数字信号处理器，用于对由计算机主机读取的数据流进行加密和解密，与通用串行总线接口芯片相连接；智能卡芯片，用于存储密钥和

个人信息，与数字信号处理器相连接；加密装置驱动器，用于获取计算机主机中文件系统对计算机硬盘的读写操作，将多组16位的硬盘数据转换为一组128位的加密解密数据，控制加密装置对128位的数据进行加密解密，置于计算机内的文件系统驱动器与硬盘驱动器之间。

当用户需要对计算机主机加密文件夹内的关键数据进行读写操作时，可将加密装置插到计算机主机的通用串行总线接口上。本发明的加密装置自动在设备层对保存到“加密文件夹”内的所有文件进行加密。数据的加密运算、密钥的使用和保存全部在与通用串行总线接口相连接的加密装置内的芯片内部进行，不进入计算机环境，因此可以完全杜绝黑客程序的跟踪和攻击。即使计算机整机丢失或被盗，也能有效防止信息泄露。

本发明的基于通用串行总线接口的计算机文件夹加密装置中，所用的通用串行总线接口芯片，使用飞利浦公司的ISP1581高速USB2.0接口器件，完全符合USB 2.0规范，用于计算机主机与数字信号处理器之间的高速数据传输和通讯。

所用的数字信号处理器，使用德州仪器公司的TMS320数字信号处理器，内部封装了标准的DES、3DES对称密码算法。对计算机主机读写数据流进行加密解密操作时，首先从智能卡芯片中读取密钥，然后执行密码算法对数据流进行加密解密。TMS320数字信号处理器运算DES加密算法时可达到每秒100Mbit的数据传输率，完全满足硬盘数据加密速度的要求。

所用的智能卡芯片，使用Atmel公司的8位AT05SC智能卡微控制器，用于存储执行密码算法所需的密钥，以及用户口令（PIN码）等个人信息。该芯片内含40KB只读储存器、2KB电可擦可编程只读储存器，具有全球唯一的64位产品序列号。初始化时用64位产品序列号作为种子，产生128位的用户加密/解密密钥，使得每把硬件钥匙内的数字密钥具有唯一性，密钥重复出现的可能性为$1/10^{38}$，保证了使用者进行身份认证时的唯一性。智能卡芯片不易伪造，可以抵御物理、电子、化学方法的攻击，使基于通用串行总线接口的加密装置具有很高的安全保密性。

加密装置驱动器，用于获取计算机主机中文件系统对计算机硬盘的读写操作信息，如盘符（C：D：等）、文件夹名、文件名和数据流等；将多组16位的硬盘数据转换为一组128位的加密解密数据；控制加密装置对128位的数据进行加密解密。加密装置驱动器置于计算机文件系统驱动器与硬盘驱动器之间，为一段运行在Windows操作系统Ring0级上的设备驱动程序，使应用程序能够在操作系统底层控制加密装置的操作。当操作系统对文件发出“写”指令时，由加密装置驱动程序拦截内存中将要进行写操作的数据流，同时调用加密装置对数据进行加密处理后存储到指定的硬盘空间。由于这种方法是动态实现加密处理，无论系统出现死机或断电，存入硬盘的数据始终是密文，使得加密文件的安全性更加可靠。最重要的是，使用者无须对文件加密解密进行任何操作，只需使用Windows操作系统原有的命令，在对文件进行保存、另存为、拷贝粘贴、拖动的过程中，计算机自动完成对文件的加/解密操作，从而可实现Windows操作系统的透明操作。

以下介绍本发明装置的工作原理和工作过程：

本发明提出了一种加密装置和密钥与计算机系统分离的加密方法，可防止计算机整机丢失或被盗时产生的信息泄露危险。用户可设置专门用于存储关键数据的加密文件夹，加密装置只对指定文件夹中的数据进行加密解密操作。

1、工作原理：

密钥的生成和注入：使用加密装置内智能卡芯片的唯一产品序列号作为种子，经Hash 算法产生 128 位的用户加密解密密钥。密钥以密文的形式存放在加密装置内的智能卡芯片中，智能卡芯片的安全保护功能可防止攻击者读取密钥信息。

由于使用了智能卡芯片内的产品唯一序列号为种子产生密钥，即使非法用户窃取了合法使用者的加密装置进行复制，每个加密装置内的智能卡芯片序列号不同，用同型号的通用串行总线接口芯片、数字信号处理器和智能卡芯片进行复制，其结果也是截然不同的，保证了加密装置硬件的不可复制性。

（1）加密装置驱动器实时监控计算机内存对硬盘的读写操作。当计算机对加密文件夹进行读写操作时，加密装置驱动器截获主机和硬盘之间的数据流；

（2）加密装置驱动器将多组 16 位的硬盘数据转换为一组 128 位的加密解密数据后，送入基于通用串行总线接口的加密装置进行加密解密；

（3）加密装置驱动器将加密装置输出的 128 位加密解密数据转换为可供计算器和硬盘读写的多组 16 位数据。

2、身份验证过程：

（1）计算机对加密装置进行身份验证：将加密装置插入计算机通用串行总线接口时，加密装置驱动器从加密装置内的智能卡芯片中读取产品序列号，判断是否为合法加密装置。

（2）加密装置对用户进行身份验证：鉴别用户身份的用户口令（PIN 码）存放在加密装置内的智能卡芯片中。将加密装置插入计算机通用串行总线接口时，加密装置驱动器提示用户用键盘输入用户口令。如果输入的口令与智能卡芯片中的相同，则通过身份验证。如果输入的口令连续三次错误，加密装置驱动程序将锁定身份验证过程。

3、用户在使用本发明的加密装置时，对文件的加密、解密操作方法：

创建加密文件夹：在每台计算机中，可创建1—20个加密文件夹。

文件加密：直接使用Windows的拷贝、粘贴、拖入、另存为等操作，将重要文件写入已设置好的加密文件夹，或直接在加密文件夹中创建文件后保存，文件都将在上述过程中自动被加密。

文件解密：直接使用 Windows 的拷贝、粘贴、拖出、从所设置的文件夹中直接打开文件或另存为，文件将在上述操作中被自动解密。

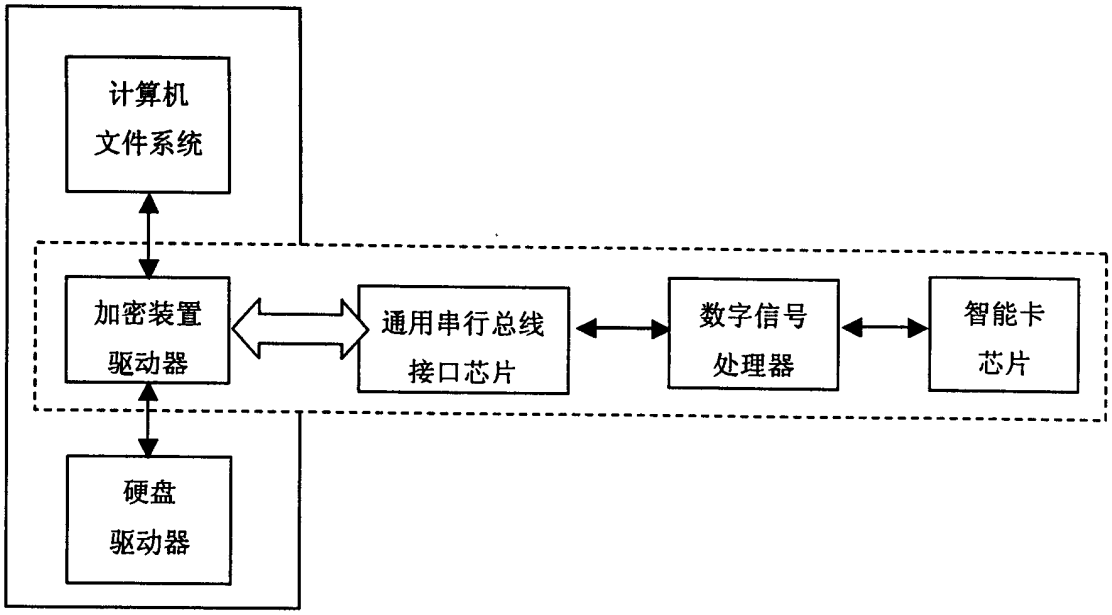


图 1