硬盘加密和身份认证的硬件实现

刘建明,贺占庄
(西安微电子技术研究所,陕西 西安 710065)

摘 要:介绍了目前流行的加密算法规则及其应用领域。通过对DES算法的硬件实现,提出了一种通过IDE接口实现加密硬盘的方案,以及U盘的身份认证方案,为用户本地信息的安全性提供了双重保障,同时相对于用户操作透明,对机器性能无任何影响。该方案目前已经进入试验阶段,基本能够较好地解决用户硬盘保密性要求和用户身份认证的惟一性要求,以期向市场进一步推广。

关键词:加密算法;身份认证;接口设计;通用串行总线
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2006)06-0139-03

A Hardware Design of Harddisk Encryption and Identification

LIU Jian-ming, HE Zhan-zhuang
(Xi'an Institute of Microelectronic Technology, Xi'an 710065, China)

Abstract: The popular encrypt algorithms are introduced in this paper. By a hardware realization of DES algorithm, a harddisk encryption precept using the IDE interface is lodged as well as the identification precept using a USB disk, which can dually ensure the customers' security in local information. At the same time, this precept is transparent for the users' operation and it does nothing to the computer's capability. This precept has been in examination at the present, and the result is that it can properly meet the request of the harddisk secret and the exclusive user identification. In the future, it will go to the market.

Key words: encrypt algorithm; identification; interface design; USB

0 引 言

随着信息时代的来临,每个人都在不自觉中被各种信息所包容,在这样一个时代,谁是信息的敏感者、先驱者,谁就获得了各方面的主动权,从而为自身赢取更多的利益。因此,个人或集体对信息的保护就显得分外重要,尤其相对于竞争者而言。在过去的若干年中,信息加密技术已经发展成为一门新兴学科,也提出了各种成熟的技术,但很难防止信息从内部的泄漏,所以文中提出了一种通过硬件加密的方法保证即使本地磁盘丢失时信息也不会泄漏,同时提供一种身份认证方法防止未授权的本地操作。

1 流行加密算法简介

数据加密技术从最初的字母置换或位置变换发展到现在已日臻成熟,现今流行的加密算法几乎是无法破解或在信息有效期内无法破解的,保障了信息的安全。下面简要介绍一下目前流行的加密算法[1,2]:

1)DES:即数字加密标准,最著名的保密密钥(或对称密钥)加密算法,是由IBM公司在20世纪70年代发展起来的,并经政府的加密标准筛选后,于1976年11月被美国政府采用,DES随后被美国国家标准局和美国国家标准协会(American National Standard Institute, ANSI)承认并给予公布。DES中密钥只有56位,对于当今的技术而言,该加密算法很容易遭到破坏和攻击。

2)IDEA:国际数据加密算法(IDEA)是由X. Lai和J. Massey于1991年开发出的一种取代DES标准的加密系统。支持对称性密码机制(加密和解密密钥相同)。和DES一样,每次允许操作8字节,但使用128位密钥提供非常强的安全性。

3)RC4:由Ron Rivest开发出来的一种RSADSI私有系统,应用于大量商业系统,如Lotus Notes和Secure Netscape。

4)RSA:一种基于陷门(Trapdoor)功能概念的加密算法,该算法中产生密钥很复杂。RSA算法的名字以发明者的名字命名:Ron Rivest, Adi Shamir和Leonard Adleman,于1977年推出。RSA算法适用于公共密钥加密和数字签名。其安全性依赖于大数的因子分解。

5)MD5:信息摘要算法5,是RSA数据安全公司开发的一种单向散列算法,MD5被广泛使用,可以用来把不同长度的数据块进行暗码运算成一个128位的数值;

另外还有用于不安全媒体上的Diffie-Hellman算法、利用RSA公共密钥算法对电子邮件进行加密处理的公共密钥系统PGP等。

收稿日期:2005-10-16
作者简介:刘建明(1982-),男,江苏人,硕士研究生,研究方向为嵌入式系统设计;贺占庄,研究员,研究方向为计算机应用与控制。

2 加密算法的比较和选择

DES 使用 56 位密钥对 64 位的数据块进行加密，并对 64 位的数据块进行 16 轮编码。于每轮编码时，一个 48 位的“每轮”密钥值由 56 位的完整密钥得出来。DES 用软件进行解码需用很长时间，而用硬件解码速度非常快[1]。

IDEA 虽然使用 128 位密钥提供了更强的安全性，但其算法复杂程度要比 DES 高一个数量级，硬件实现当然也就复杂很多，限制了编解码速率，因此，考虑到本方案的实现要对机器性能无影响，最终选择 DES 算法进行硬盘数据加密。

根据 MD5 单向散列算法的特性，将其应用于密钥的保护以防止对 U 盘的数据反读获取密钥；用户设定密码后，经 MD5 算法器将设定密码和一些其他认证信息一起计算出惟一的 128 位数据保存于 U 盘，供下次输入密码时的检测。

3 硬盘加密和身份认证方案实现

本设计包含以下几个模块：ASIC 信号控制中心模块，USB 状态检测模块，加密算法实现模块，MD5 身份认证模块，其逻辑结构如图 1 所示。

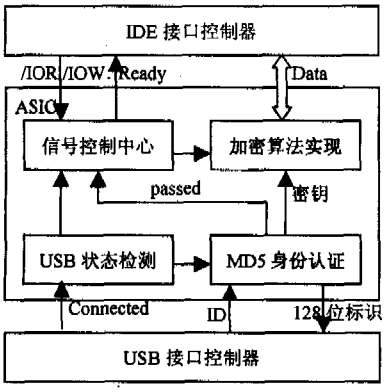

图 1 硬盘加密和身份认证逻辑图

3.1 各模块功能介绍

3.1.1 ASIC 信号控制中心模块

该模块负责与 IDE 接口控制器的信号交互，以及控制整个 ASIC 内部各信号间的交互。当检测到 IDE 接口控制器的数据读或写信号有效时，该控制中心询问 USB 状态检测模块当前是否有 U 盘插入，如果有 U 盘插入，接着读取 MD5 身份认证模块的认证有效信号，当用户认证被通过之后，控制中心告知 IDE 接口控制器可以返回 IO_CH_RDY 有效信号，同时给加密算法实现模块一个有效信号，随时进行硬盘数据的读写操作。

3.1.2 加密算法实现模块

该模块实现要写入硬盘的数据的加密和需从硬盘读取的数据解密操作，采用 DES 加密算法实现，密钥由 MD5 身份认证模块获取。此加密算法的实现可以避免硬盘被盗用时数据的保密性。

在实现数据加解密时，该模块采用多级寄存器方式，一级寄存器用于存放明文；二级寄存器在加密过程中存放临时生成数据；三级寄存器存放加密完成后生成的密文。解密过程类似，只是解密操作将三级寄存器作为源操作数，一级寄存器作为目的操作数。此方案的实现便于数据与外界的交互：需写入硬盘的或要从硬盘读取的明文数据直接与一级寄存器交互，而实际写入到磁盘的密文数据则来源于三级寄存器，从磁盘读取密文数据也直接送交三级寄存器进行解密。

3.1.3 USB 状态检测模块

该模块检测当前有没有 U 盘插入（读取 USB 接口控制器相关状态位），有 U 盘插入时给信号控制中心提供一个有效信号，同时给 MD5 身份认证模块发一个有效信号开始身份认证。

3.1.4 MD5 身份认证模块

该模块使用 MD5 算法进行身份认证，当 USB 检测模块发送一个连接有效信号后，认证模块就提示用户输入密码，然后将输入的密码和 U 盘的产品序列号一起计算出一个 128 位的哈希值，再将该值与保存于 U 盘中的 128 位标识进行对比，如果一致则说明用户对硬盘的操作获得许可，给信号控制中心发送一个认证通过信号，同时提取这 128 位中 56 位作为 DES 算法的密钥发送给加密算法实现模块；如果认证失败，则用户无权访问硬盘，使机器一直处于等待状态。在授权用户使用机器期间可以重新设定密码，当新密码确认时，由该模块重新计算一个 128 位标识并将其保存于 U 盘中供下次校验。

3.2 ASIC 与 IDE 接口控制器连接

目前 IDE 接口标准主流是 UDMA/66（66.67MB/s），作用是连接硬盘和光驱[3]，其接口使用 40 个引脚，其中 DD0－DD15 用来进行数据传输，/IOR，/IOW 接受主机发来的硬盘读写信号，IO_CH_RDY 告知主机硬盘已准备好进行数据传输[4,5]，其它一些信号于本设计无关，故不做介绍。ASIC 与 IDE 接口控制器的连接如图 2 所示。

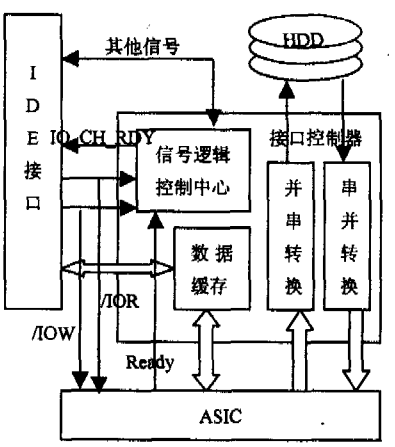

图 2 ASIC 与 IDE 接口控制器连接图

本 ASIC 设计模块获取来自 IDE 接口的硬盘数据操作信号，在身份认证通过后给 IDE 接口控制器一个 Ready 信号告知其可以进行硬盘数据操作；ASIC 设计模块中一级寄存器与原 IDE 接口控制器中数据缓存器相连，三级寄存器与其串并转换模块和并串转换模块相连，由硬盘操作信号控制：/IOW 有效时并串模块当前有效，发送密

文,/IOR 有效时串并模块当前有效,读取密文。同时在原 IDE 接口控制器中断开数据缓存与数据转换模块的连接。

从以上的 ASIC 与 IDE 接口控制器连接图可以看出,对原 IDE 接口控制器只做了极小的一部分修改,简化了硬件设计复杂性;对外,还保持标准 IDE 接口,为本设计提供了应用方便性和用户操作的透明性;ASIC 三级寄存器的设计保证了数据传输的流畅,一次数据传输只相对于原标准接口控制器控制下延迟 2 个数据周期,对机器性能几乎无影响。

3.3 U 盘的使用

USB,即通用串行总线,现已广泛应用于 PC 领域。USB 以其可以热插拔和重量轻等优点赢得了广大用户的青睐,因此本设计中采用 U 盘作为身份认证的一个载体,方便使用。

用作身份认证的每个 U 盘包含有惟一的产品序列号信息,它与用户输入的密码一起进行哈希计算,生成惟一的 128 位标识供 ASIC 身份认证。

当用户要求使用本地机器时,必须插入身份认证 U 盘,同时输入密码,经验证通过后方可使用;若用户因事离开时,拔出 U 盘随身携带,此时 ASIC 中 MD5 身份认证模块则发送一个身份认证无效信息,终止一切硬盘操作,等待下一次重新身份认证成功。此方案的实施可以避免同事或其他一些未经同意的本地计算机操作,保证了用户信息的隐秘和不受侵犯。

4 软件设计流程

软件设计流程如图 3 所示,用户开机后首先检测有没有身份认证 U 盘插入,在检测到有 U 盘时提示用户输入密码,由硬件进行身份认证,认证通过后才能进入操作系统进而进行别的一些硬盘访问操作,否则不能进入系统。在认证过程中,如果认证失败,则提示用户重新输入密码(无论是密码错误还是 U 盘错误),在三次认证失败之后则进入等待状态,等待重新插入 U 盘。如果用户在正常操作过程中有密码修改请求,则将密码修改后生成的 128 位哈希标识回写入 U 盘。当检测到 U 盘被拔出时,系统同样进入等待状态。

5 结束语

本设计采用 U 盘外加密码输入的身份认证方案来保证用户信息安全,但如果用户忘记密码也会为自己的操作带来很大的不便;现今国际上流行很多的生物活性检测技术可以消除忘记密码的后顾之忧。因此本设计将来也可升级为生物活性认证,只需将原来的密码体制做修改即可,升级非常方便。

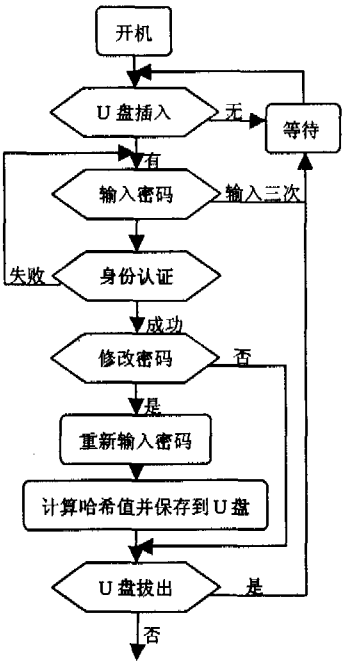

图 3　软件设计流程图

参考文献:

[1] 段云所. 数据加密算法[R]. 北京:北京大学计算机系,2005.

[2] 曲英杰,刘卫东,战嘉瑾. 可重构密码协处理器指令系统的设计方法[J]. 计算机工程与应用,2004(2):10-13.

[3] 和　嘉. IDE 接口[EB/OL]. http://www.pp51.com/za/300/data/IDE%20.mht,2005.

[4] 索远强,周国祥,苗玉彬,等. 智能测量系统中的海量数据存储技术[J]. 电子技术应用,2005(5):21-24.

[5] 潘向峰,岳春生. Xscale PXA255 处理器与 CF 卡的接口设计[J]. 电子工程专辑,2005(5):18-22.

(上接第 9 页)

本方案的突出特点是它以菜单命令的输入状态为基础对按键进行处理,它能很好地满足未来应用提出的新需求,便于键盘功能扩充,提高了控制软件的可维护性。该处理方案具有一定的通用性,有较好的应用价值。整个车流量控制软件在模拟环境下的调测试结果表明,文中提出的键盘处理方案不会影响其它的处理,能很好地满足项目的需求。

参考文献:

[1] 戴梅萼,史嘉权. 微型计算机技术及应用(第 2 版)[M]. 北京:清华大学出版社,1996.

[2] 龚建伟,熊光明. Visual C++/Turbo C 串口通信编程实践[M]. 北京:电子工业出版社,2004.

[3] ATMEL. AT45D041 技术文件[EB/OL]. http://www.atmel.com,2005.

[4] 王德宪. 用四个按键向单片机系统输入数据的方法[J]. 电子世界,2002(8):31-32.

[5] 曹国辉. 基于状态分析的键盘管理软件设计[J]. 单片机与嵌入式系统应用,2002(6):17-20.

[6] 钱　能. C++语言程序设计[M]. 北京:清华大学出版社,1999.