文章编号:1674-2869(2012)2-0067-04

嵌入式安全存储系统的研究

罗 肖[1,2],刘 军[1,2],杨 辉[1,2]
(1. 武汉工程大学智能机器人湖北省重点实验室,湖北 武汉 430074;
2. 武汉工程大学计算机科学与工程学院,湖北 武汉 430074)

摘 要:经过分析嵌入式系统的安全需求,描述了一种基于微型加密算法的USB安全存储系统的系统构造,采用微型加密算法来对USB设备进行数据安全存储. 以芯片CY7C68013为主控芯片,嵌入式系统开发板固件采用USB接口直接下载,采用智能仿真设备进行在线调试. 实验表明加密处理的数据基本不影响USB数据的读取操作,此嵌入式平台能够实现相对的安全性能,具备低成本、低功耗和结构简单等优势.

关键词:安全存储;改进型微型加密算法;USB2.0;嵌入式系统
中图分类号:TP37 **文献标识码**:A **doi**:10.3969/j.issn.1674-2869.2012.2.016

0 引 言

USB移动存储设备由于其方便小巧,易于携带,具备了防磁、防震、防潮的等诸多优点得到使用者广泛的好评. 同时,以USB接口为传输通道的方法使得该类设备具备传输速度快、使用方便、可热插拔等特点,拥有良好的市场. 但是从“艳照门”等系列个人隐私泄露的事情来看,发现USB存储设备必需加强数据的安全性. 市场常见加密型U盘主要分为普通口令认证型、软件加密型和硬件加密型,而主流的加密USB存储设备均采用安全级别较高,数据加密速度快,但是其硬件加密的实现需要用到价位较高的专用芯片,推高了USB存储设备的价格. 例如,文献[1]就采用基于FPGA(现场可编程门阵列)的USB移动硬盘硬件加密方案,将智能卡的功能与USB移动硬盘的功能结合的安全设计方案. 文献[2]则选用中兴的Z32UF芯片实现了加密U盘的系统原型UDisk(移动磁盘),该系统能支持多种国家认证的加密算法,如SSF33、SCBZ等,扩展性较强. 文献[3]则采用单片机CY7C68013和安全Flash(闪存)芯片X76F640实现了集数据加解密、认证于一体的加密U盘,该U盘的信息加密采用AES(高级加密标准)算法,通过安全Flash芯片保存用户密钥,硬件电路比较复杂. 针对嵌入式系统[4]在安全与性价比这一问题上的权衡,发现其实可以选用CY7C68013芯片配以XXTEA(一种微型分组加密算法)加密算法就能很好的解决这一问题. 为此,通过研究在CY7C68013芯片平台下,针对USB安全存储系统中实现一个基于XXTEA加密算法的USB存储设备实现安全存储的功能. 最后,给出了具体硬件平台环境下的采用安全加密和未采用安全加密的设备访问测试结果对比.

1 USB安全存储设备的系统构造

本USB安全存储设备系统采用USB接口控制芯片,并以该芯片为控制中心,结合CF(闪存存储卡)存储卡和安全存储设备的存储接口、访问安全特性,设计实现对USB存储设备使用认证、口令管理、存储载体安全保护,并对数据存储底层设备进行加密和存储管理. 其概念图如图1所示,硬件层由USB接口控制芯片和CF存储卡构成;固件层则在硬件基础上实现USB与主机通信、系统控制、存储接口和加密解密安全管理;接口层在Windows系统中提供应用接口、驱动开发和存储与安全管理.

为了控制成本,USB安全存储设备系统采用USB接口控制芯片通过固件实现口令保护载体密钥、数据有效期等安全参数,加密算法采用XXTEA算法,并设计存储数据完整性校验.

收稿日期:2011-12-02
基金项目:武汉工程大学大学生校长基金项目;武汉工程大学大学生教育创新基金项目
作者简介:罗 肖(1992-),男,湖北武汉人. 研究方向:信息系统开发与应用,USB安全存储系统技术.
指导老师:刘 军,男,副教授,博士,硕士研究生导师. 研究方向:嵌入式系统开发与应用,基于网络的存储系统.

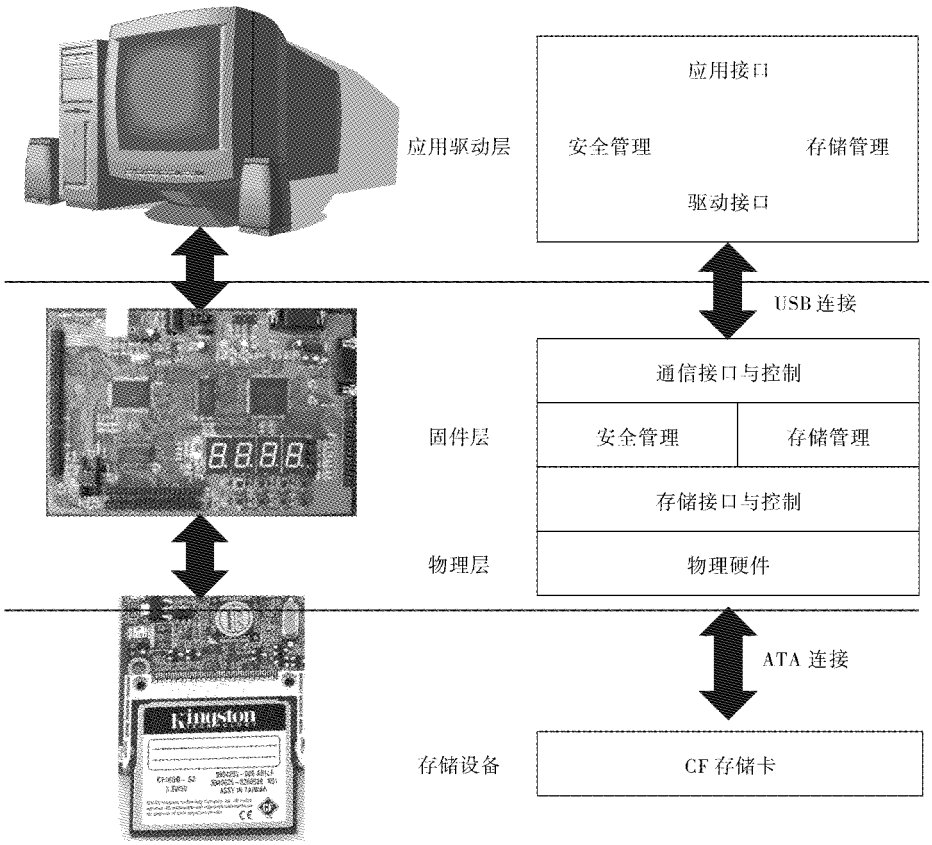


图1 USB安全存储设备系统模型图

Fig. 1 USB secure storage system model

2 USB安全存储设备的加密算法分析

数据加密算法主要分对称密钥与非对称密钥两种类型,根据两种算法类型的特点的不同,其应用领域也不尽相同. 对称加密算法主要应用于数据块加密,因为一般的对称数据加密算法的特点就是加密解密速度快,吞吐量大,而且易于硬件实现. 而非对称数据加密算法的特点是加密算法的安全性能高,但是加密解密算法计算量特别大,因此广泛应用与数据签名等安全领域. 本USB安全存储设备系统采用的XXTEA算法是一种对称密钥加密算法. 该类加密算法是从TEA算法(分组加密算法)改进而来,其中TEA算法[5]由剑桥大学Wheeler D J和Needham R M首先提出,TEA算法采用128位bit(16 byte)作为密钥,每一次可以操作8个字节的数据,通过数据迭代计算加密,文献[5]要求迭代轮数最少32轮,并推荐的迭代轮数是64轮. TEA算法自推出以来由于实现简单,加密解密速度快,得到了广泛的应用,但是文献[6]指出TEA算法的密钥表可以被攻击,并提出改进的XTEA算法,该算法采取不正规的方式将4个子密钥混合处理. 文献[7]提出的Block TEA算法进一步改进XTEA轮循函数,不仅将轮循函数作用于块内的数据,同时应用与相邻的数据,实现对任意32位长度的数据块进行加解密的操作. Needham R M最终改进了自己提出的TEA算法并提出XXTEA算法[8],该算法处理数据块时不仅利用相邻数据块(类似于Block TEA算法),同时改进XTEA轮循函数,采用二输入量的MX函数,提高算法的抗攻击能力,相比较TEA算法来说,XXTEA算法的6轮加密次数所需算法攻击的明文数据量由234提高至280,在提高安全性能(排除暴力攻击的可能性)的同时不降低加密解密的处理速度.

这里给出XXTEA算法的一轮加密过程的图示,如图2所示,其中⊕表示异或,⊞表示求和,>>表示右移,<<表示左移. 改进的XXTEA算法是根据加密的数据长度来确定其加密迭代轮次,而根据文献[8]的要求加密轮次至少为6轮,最多可以为32轮. 因此,可以发现XXTEA算法主要包括异或、加法和移位等运算,它的结构非常简单,只需要执行异或、加法和移位等运算的硬件即可快速实现加密解密算法,且软件实现的代码可以用C语言或者汇编语言实现,算法短小精悍,具有良好的可移植性,非常适合嵌入式系统应用. 综

合 XXTEA 算法的优点,它可以很好地应用于本 USB 安全存储系统.

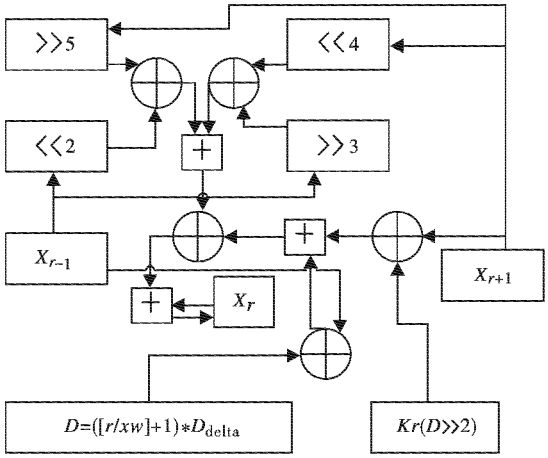


图 2　XXTEA 算法的一轮加密过程

Fig. 2　One round of XXTEA algorithm

3　USB 安全设备系统的加密解密流程

如图 1 所示,USB 安全设备系统中,固件层加密解密模块处于 USB 接口与 ATA 接口(嵌入式接口)之间,必须对 CF 存储卡的命令、数据与状态进行分类,并根据实际情况进行分类,对需要加密的数据,并调用加密模块进行相应的加密操作,对需要解密的数据则需要调用解密模块进行相应的解密操作. 因此,对 IDE 接口(电子集成驱动器)的 ATA 协议命令解析模块和传输控制模块就非常重要. 因为,ATA 协议命令解析模块负责实现对 IDE 接口的主机的命令解析过程,从而识别出每条命令的基本信息. 传输控制模块则负责对主机的控制信号进行命令响应,从而管理硬盘控制期于主机之间的数据传输过程.

USB 安全系统在具体实现上是对整盘的加密,暂时还未涉及目录与存储对象细颗粒的加密操作. 因此,对于具体加密解密处理的命令分类情况来看,从 ATA/ATAPI - 7(IDE 设备的相关标准)协议中的每条命令分析可以得到命令代码及其相应的传输类型和传输模式,以及在该条命令下传输的数据加密/解密与否的判断. 在 PIO(程序输入输出模式)传输模式下,写命令代码为 0xC5h 需要进行加密处理,而同类模式下读命令代码为 0xC4h 需要进行解密处理;在 Ultra - DMA(高速直接内存存取)传输模式下,写命令代码为 0xCAh 需要进行加密处理,读命令代码为 0xC8h 需要进行相应的解密处理. 对于大部分命令的下传的数据均不需要加密/解密处理,一般为直通处理.

USB 安全系统的设备接口及核心控制模块芯片采用的是 Cypress 公司的 CY7C68013 芯片. 该芯片是一款全速 USB 控制器,内嵌一个增强型的 8051CPU. 在整个安全系统中,CY7C68013 芯片担当了 USB 内核与主机通信、传输数据、加密解密存储数据等重要工作. 其具体工作流程如下:

a. 给系统设备上电,启动系统固件,USB 系统按照 USB 规范应答主机,并提供本 USB 设备的标识.

b. USB 设备枚举本系统设备,并加载相应的驱动,在驱动加载完成之后将控制权转给内核中 8051CPU.

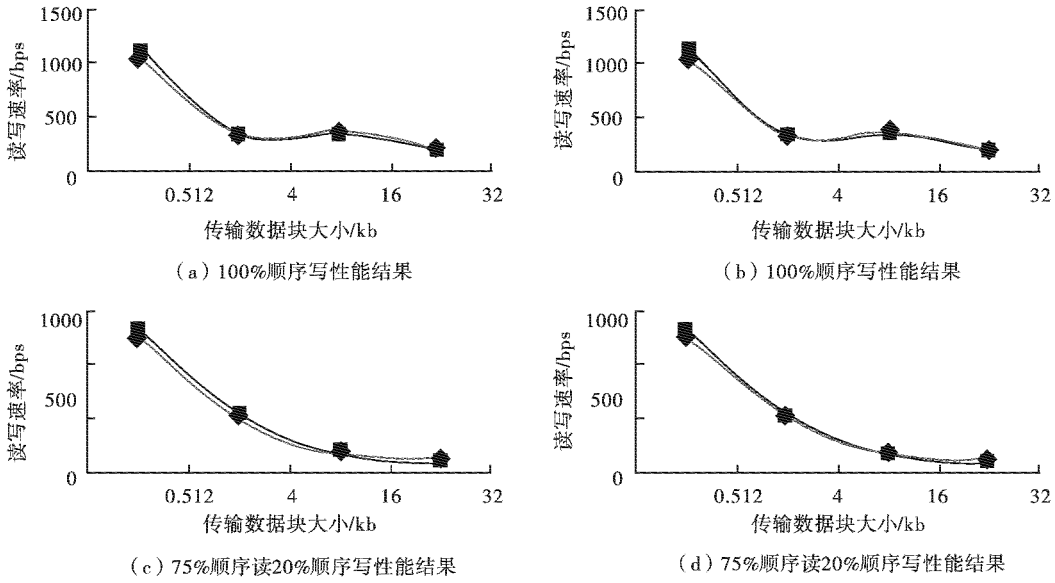
c. 8051CPU 与主机交互,验证用户身份.

d. 用户身份通过后,提取相应的安全密钥,对存储芯片的数据进行加密/解密处理.

4　实验环境和实验分析

系统测试主机是一台安装有 Windows XP SP3 系统的 Intel Core(TM)2 Duo 处理器的 PC 机. 本安全存储系统由一块基于 CY7C68013 芯片的开发板和 CF 存储卡(包括 ATA 连接设备)构成. 基于 CY7C68013 芯片的开发板固件编程与调试采用 USB 接口直接下载和调试,同时也采用 smart ICE(并口微处理器仿真器)进行在线调试.

为了测试虚拟 U 盘的读取性能,因而采用 Iometer 软件对未加密的 USB 存储系统和使用加密的 USB 安全存储系统分别进行了测试,同时为了删除测试系统中读写负载对测试数据的影响,整个测试环境要求测试时不发生其他程序读写 USB 存储系统的情况,测试数据块大小为 0.512 kb,4 kb,16 kb,32 kb,分别进行了时间段为 2 min 的顺序读取和写入等两个方面的测试,其对比结果如图 3 所示,安全 USB 存储系统中的加密后 U 盘的速率与未加密的 U 盘的访问速率基本一致,显然经过加密后的数据造成的对数据读写性能的影响很小. 通过对数据的分析,可以发现经过加密处理的数据基本不影响 USB 数据的读取操作,因此,可以认为 XXTEA 加密解密算法在安全 USB 存储系统得到了较好的应用.



(a) 100%顺序写性能结果　(b) 100%顺序写性能结果

(c) 75%顺序读20%顺序写性能结果　(d) 75%顺序读20%顺序写性能结果

图3　顺序读取速率性能比较图

Fig. 3　Sequential read rate performance test results

注:—◆—未加密; —■—加密

5　结　语

USB存储设备有着良好的市场和口碑,但是USB存储设备期待加强数据的安全防护. USB存储设备的安全技术正日益发挥其重要作用,但是对于常见的加密型U盘中普通口令认证型安全性能相对较弱,软件加密型依赖于计算机主端的安全性能,而硬件加密型则需要用到价位较高的专用芯片,推高了USB存储设备的价格. 本文从USB存储设备的安全与性价比的角度出发,给出如何在通过在USB存储系统中设计实现一个基于存储设备的固件加密解密方法,实现在USB设备固件级别的安全存储系统的功能. 最后给出了相应的测试性能分析,说明本文给出的方法基本不影响存储设备的读写吞吐率. 通过系统性能测试分析,可以发现数据传输随着传输数据块大小性能有所下降,因此,下一步的研究方案将逐步改进以提高嵌入式系统性能从而提高安全USB存储系统的数据传输率.

参考文献:

[1] 胡伟,慕德俊,刘航,等. 移动硬盘硬件加密的设计与实现[J]. 计算机工程与应用,2010(22):62-64.

[2] 付积存. 安全U盘嵌入式系统的设计与实现[D]. 武汉:华中科技大学,2006.

[3] 易青松,苏锦海,岳云天,等. 基于CY7C68013安全U盘的硬件设计[J]. 计算机工程与设计,2007,28(6):297-299.

[4] 盛李立,王忠,王春丽,等. 基于SPI接口的无线网卡设备驱动设计[J]. 武汉工程大学学报. 2011,33(6):89-97.

[5] Wheeler D J, Needham R M. A Tiny Encryption Algorithm[C]//Fast Software Encryption. Published in the proceedings of that workshop, 1994:363-366.

[6] Needham R M, Wheeler D J. Tea extensions[R/OL]. http://www.movable-type.co.uk/scripts/xtea.pdf. 2010-07-22.

[7] Saarinen M. Cryptanalysis of block tea[R/OL]. http://www.cc.jyu.fi/mjos/block_tea.ps. 2010-07-22.

[8] Needham R M, Wheeler D J. Correction to xtea[R/OL]. http://www.movable-type.co.uk/scripts/xxtea.pdf. 2010-07-22.

(下转第73页)