基于 FPGA 技术的 GPS 数据加密系统设计研究

邢红涛,王建功,初 晓

(中国人民解放军 63895 部队,河南 孟州 454750)

摘 要:针对 GPS 测量系统数据传输过程中的安全问题,采用 FPGA 技术设计了 GPS 数据加密系统。系统移植 MD5 算法到 NIOS 中对系统口令加密,并设计 DES IP 对 GPS 数据加密。实验表明,该设计可有效防止 GPS 数据被非法窃取,具有安全性强、速度快、操作简便等特点。

关键词:FPGA;GPS;MD5;DES;数据加密

中图分类号:TP309.7 **文献标识码**:A **文章编号**:1674-7720(2010)15-0080-03

Research and design of the GPS data encryption system based on FPGA technology

XING Hong Tao, WANG Jian Gong, CHU Xiao

(Unit-63895 of PLA, Mengzhou 454750, China)

Abstract: Focusing on the security problem in the data transmission process of GPS measurement system, the GPS data encryption system is designed using FPGA technology. The system transplants MD5 algorithm into NIOS to encrypt the system password and designs DES IP to encrypt the GPS data. Experiment shows that this design could effectively prevent the GPS data from being illegally robbed, with characteristics of strong security, fast speed and simple operation.

Key words: FPGA; GPS; MD5; DES; data encryption

随着网络通信技术的发展,数据传输对安全性的要求也随之加强。如何确保信息的正确认证与严格保密,保证数据信息在传输与处理过程中不被非法窃取和篡改,成为信息安全理论与技术研究的重要内容。多数情况下,数据加密是保证信息机密性的惟一方法。在 GPS 测量系统中,GPS 定位数据以明文形式通过电台进行传输,可能会被同型号电台获取,存在一定的安全隐患。本设计应用 FPGA 技术设计了 GPS 数据加密系统,通过 MD5 加密算法对管理员口令进行加密;DES 加密算法对 GPS 数据进行加密。这样,GPS 数据经加密卡加密后再以密文方式发给电台进行传输,同时接收端必须使用密钥将密文解码才能得到定位数据,从而确保了数据传输的安全。

1 系统组成及功能

GPS 数据加密系统由机载模块和服务器端两部分组成,通过电台进行通信。其系统结构如图 1 所示。

1.1 机载模块

机载模块由 4×4 键盘、机载 LCD、加密卡三部分组成,用户可通过 4×4 键盘发送预定义指令、更改密钥等操作;机载 LCD 用于显示系统工作状态、飞行参数等数

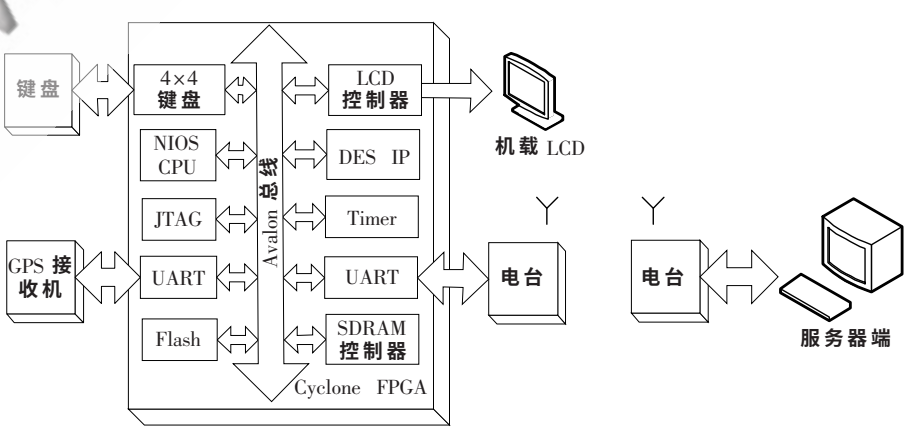

图 1 GPS 数据加密系统示意图

据;加密卡为系统核心部件,主要有以下4个功能:

(1)解析、处理GPS数据、检测设备工作状态并在LCD上显示相关信息;

(2)接收GPS数据并通过加密卡对其加密,将密文通过电台传送到服务器端;

(3)处理键盘或服务器端输入的预存指令编号或新指令,将指令发给GPS接收机并返回回馈信息;

(4)更新键盘或服务器输入的新密钥或新管理员口令。新密钥先保存在Flash中,再通过总线传给密钥寄存器;新口令保存在Flash中。

系统工作时,加密卡通过UART IP获取GPS数据后同时传给NIOS和DES IP。NIOS解析GPS数据并经LCD Controller传给机载LCD进行实时显示,方便机上人员了解设备工作状态;DES IP将GPS数据加密后,通过I/O中断传给NIOS,NIOS将密文加入数据包头、尾字节后,再经电台传到服务器端。

1.2 服务器端

服务器端为通用计算机,其应用软件使用VC++6.0开发,服务器的主要功能有以下6点:

(1)接收电台传来的密文并进行DES算法解密、解析和处理GPS数据;

(2)显示GPS参数,并保存数据;

(3)发送GPS接收机控制指令;

(4)更改密钥;

(5)更改管理员口令;

(6)设置串口参数。

2 数据加密算法的原理及应用

2.1 MD5算法的原理及应用

信息—摘要算法MD5(Message-Digest Algorithm 5),在90年代初由Rivest设计发明,经MD2、MD3和MD4发展而来。其作用可使大容量信息在用数字签名软件签署私人密匙前,被"压缩"成一种保密的格式(对任意长度的信息,生成一个长度为128 bit的值)。

本设计将MD5算法移植到NIOS中,用于加密管理员口令。这样系统在并不知道管理员口令的明码情况下就可以确定口令的合法性,从而有效地防止了反编译等技术手段对管理员口令进行破解。系统工作时,NIOS预先将管理员口令加密后,将MD5值存储在Flash中,当加密卡接收到更改密钥、更改口令或发GPS接收机控制指令等操作命令时,先将输入的口令计算成MD5值,然后与存储在Flash中的MD5值进行比较,如果两值相同则说明口令正确,再进行相应的操作。

2.2 DES算法的原理及应用

DES(Data Encryption Standard)是一种分组乘积加密算法,是用64 bit的密钥对64 bit的明文加密,64 bit密钥中每8 bit有一奇偶校验位不参与运算,有效密钥只有56 bit。同时,它又是对称加密算法,其加密和解密运算过程完全相同,只是在迭代运算时子密钥的使用顺序不同[1]。如图2所示,64 bit的明文块在经过初始IP置换后,被重新排列,然后进入16轮的迭代运算;每一轮迭代运算由一个f函数完成;最后一轮迭代的输出为64 bit,将其左半部分和右半部分互换产生预输出;预输出再与逆初始置换IP^{-1}作用产生64 bit的密文,IP^{-1}是IP的反变换[2]。

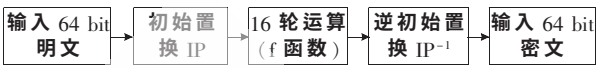

图2 DES算法总流程

采用软件方式实现的DES算法会在很大程度上占用系统资源,造成系统性能的严重下降,而DES算法本身并没有大量的复杂数学计算(如乘、带进位的加、模等运算),在加密、解密过程和密钥生成过程中仅有逻辑运算和查表运算。因而,无论是从系统性能还是加、解密速度的角度来看,采用硬件实现都是一个理想的方案[3]。

图3为DES IP的硬件逻辑图,主要由状态控制器、子密钥生成器、DES算法运算器三部分组成。其中,状态控制器用于控制IP的工作状态、模式和标识完成状态;子密钥生成器将56 bit密钥分成两部分,每部分按循环移位次数表移位并按置换选择表置换,从而生成每一轮次运算的子密钥$K(K_1, K_2, \cdots, K_{48})$;DES算法运算器为整个IP的关键,它将64 bit中间数据分为左右两部分,分别记为L_i和R_i。单个运算的过程可以写为下面的公式:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

f函数是DES算法运算器的核心。其中,$f(R_{i-1}, K_i)$功能由以下4步完成:

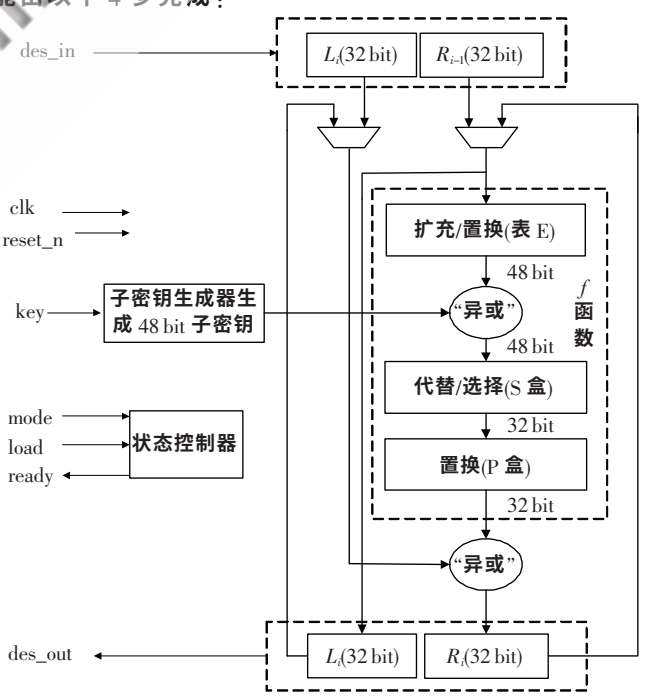

图3 DES IP硬件逻辑图

(1)将 R_{i-1} 按照扩展换位表 E 扩展为 48 bit 的数据;

(2)将扩展后的 R_{i-1} 与循环移位后的 48 bit 子密钥 $K(K_1, K_2, \cdots, K_{48})$“异或”;

(3)将“异或”后的结果送入 8 个 S 盒(S box)进行替代运算,每个 S 盒都有 6 bit 输入、4 bit 输出,并且 8 个 S 盒都不相同,48 bit 的输入分为 6 位一组,分别送到 8 个 S 盒选择相应的输出,结果为 32 bit;

(4)S 盒替代后的 32 bit 结果依照 P 盒(P box)进行置换,置换后结果即为 $f(R_{i-1}, K_i)$ 的最终值,这样便完成了 f 函数的运算。

算法中用到的初始换位表 IP、放大换位表 E、替代函数表 S、换位函数 P、逆初始换位 IP^{-1}、密钥循环移位表可在参考文献[4]中查到。本设计中,GPS 数据的加密在加密卡中完成,解密在服务器端完成,为方便功能扩展,在加密卡中设计、保留了解密功能。

2.3 DES 算法仿真验证

本设计的 DES IP 采用 ALTERA 公司的 Quartus 7.0 软件开发及 Verilog HDL 语言编写[5],整个加密卡在单片 Cyclone 系列 EP1C6Q240C8N 芯片上实现。图 4 为 Quartus 7.0 开发软件下 DES IP 的仿真图。

各仿真信号的意义及说明如下:

时钟信号(clk):周期为 10 ns、占空比为 50%;

复位信号(reset_n):低电平有效,置高;

模式信号(mode):加密/解密选择,‘1’为加密,‘0’为解密;

加载信号(load):高电平有效,置高;

加密数据(des_in):8000 0000 0000 0000;

密钥信号(key):0000 0000 0000 0000;

加密结果(des_out):95F8 A5E5 DD31 D900;

加密完成信号(ready):在第 17 个周期后置高。

DES IP 工作时,“密钥”保存在总线接口的密钥寄存器中,“加密数据”由 NIOS 输入,加密完成后,通过“加密完成信号”产生的 I/O 中断传回给 NIOS。图 4 中,其加密结果与 XILINX 公司网站上设计参考中给出的数据一致,表明 DES IP 设计正确。

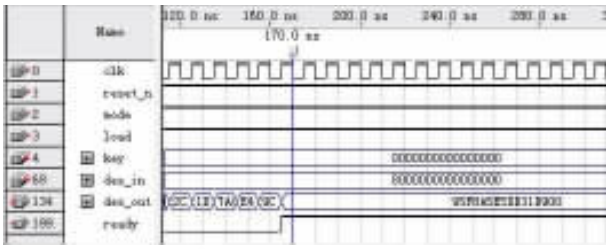

图 4 DES IP 仿真图

本设计采用 FPGA 技术设计了 GPS 数据加密系统,重点介绍了机载模块中 DES IP 的设计。实验发现,采用 NIOS 进行 DES 算法软件加密时速度慢,会出现间隔丢失 GPS 数据的现象,而采用硬件 DES IP 进行加密处理时,完全可以满足 GPS 接收机的速度需要,不会出现丢点现象。系统采用 MD5 算法对管理员口令进行加密,进一步增强了系统的安全性,因此本设计对解决该 GPS 测量系统安全性方面有较大的现实意义和实用价值。

参考文献

[1] 胡向东,魏琴芳.应用密码学[M].北京:电子工业出版社,2006.

[2] 贺雪晨,陈林玲,赵琰.信息对抗与网络安全[M].北京:清华大学出版社,2006.

[3] 褚雄,王子敬,王勇.一种基于 FPGA 的 DES 加密算法实现[J].江南大学学报(自然科学版),2006,15(6):661-664.

[4] STALLINGS W.密码编码学与网络安全(第 3 版)[M].刘玉珍,王丽娜,傅建明,等译.北京:电子工业出版社,2004.

[5] 徐光辉,程东旭,黄如.基于 FPGA 的嵌入式开发与应用[M].北京:电子工业出版社,2006.

(收稿日期:2010-01-13)

作者简介:

邢红涛,男,1982 年生,硕士,主要研究方向:检测技术与自动化装置。