

基于安全加密算法的数字逻辑仿真实验平台

付秀伟, 高兴泉, 付 莉

(吉林化工学院 信息与控制工程学院, 吉林 吉林 132022)



摘 要:为形成计算机专业特有的“数字逻辑”课程实验体系以及解决硬件基础课程之间和专业课程衔接差、课程工程实训薄弱的问题,提出一种基于安全加密算法的数字逻辑仿真实验平台。以 S-DES 加密算法安全系统为例,介绍 S-DES 加密算法原理,利用 Quartus II 仿真软件平台建立图形化加密算法模型,同时利用 Visual C++ 开发平台程序化实现算法,分别进行系统仿真验证,相互校验仿真结果。实验表明,通过引入专业知识、以工程角度实现硬件基础课程实验内容,可增强实验课程内容层次性,有效提升学生工程实践意识。

关键词:数字逻辑; 加密算法; 实验平台; 仿真软件

中图分类号:TP 302 **文献标志码:**A

文章编号:1006-7167(2017)05-0106-04

Simulation Experiment Platform for Digital Logic Based on Secure Encryption Algorithm

FU Xiuwei, GAO Xingquan, FU Li

(College of Information & Control Engineering, Jilin Institute of Chemical Technology, Jilin 132022, Jilin, China)

Abstract: In order to realize experimental teaching system of “digital logic” course for computer major and resolve the problems with poor cohesion among hardware basic courses and professional courses, and weakness in engineering training, a digital logic simulation experiment platform based on secure encryption algorithm is proposed in this paper. Taking S-DES encryption algorithm secure system as an example, the principle of S-DES is introduced, and a graphical model of encryption algorithm is built by using Quartus II. In addition, the algorithm is programmed by using Visual C++. Simulation results are compared for the two methods. Experiments show that level of experiment course content and students’ consciousness of engineering practice are enhanced by introducing professional knowledge and implementing hardware basic experimental content with project idea.

Key words: digital logic; encryption algorithm; experiment platform; simulation software

0 引 言

“数字电路与逻辑设计”课程是高校计算机专业必修的一门硬件基础课程^[1],也是专门为大二计算机专业学生量身定做的课程之一。其课程内容着重于逻

辑抽象又应用于工程实践^[2],但又区别于其他电子类专业“数字电子技术”课程的培养要求。从计算机专业学生的培养方向而言,更立足于培养计算机专业的学生掌握逻辑器件设计到计算机系统设计的全过程,进而掌握计算机硬件系统结构、工作原理,设计数字系统中时序和组合逻辑电路^[3]。在逻辑分析和电子电路两方面^[4],数字逻辑课程更侧重逻辑分析,为后续“计算机组成原理”课程做良好的知识储备。由于教学内容与数字电子技术相似度较高,实验内容基本相同,导致无法正确培养计算机专业学生的逻辑分析能力。

收稿日期:2016-09-10

基金项目:吉林省教育厅项目(20140352);吉林省科技发展计划项目(20150520114JH)

作者简介:付秀伟(1983-),男,山东新泰人,硕士,讲师,研究方向为嵌入式系统及电子技术。

Tel.: 15044660536; E-mail: fxw7720268@163.com

随着可编程逻辑技术的不断发展,EDA 技术也脱颖而出,将 EDA 技术引入数字逻辑课程实验教学中是必然的,但也急需选择适合于数字逻辑实验课程学时和培养目标且具有层次性、扩展性、灵活性的实验内容,同时设计内容要为后续硬件基础课程及专业基础课程打下基础,本文以 S-DES 安全加密算法仿真实例为例,利用 Altera 公司的 Quartus II 仿真平台搭建系统模型,将简单易行的组合逻辑电路及设计模块成功结合,从而熟练掌握 EDA 技术的数字系统设计方法,另外,在开放式实验教学过程中,学生可预先利用大一学到的 C 语言进行算法测试及验证,加强课程紧密性,也让学生辨识软件和硬件的区别^[5]。

S-DES 加密算法原理简单,一直作为“计算机网络安全”和“云计算”专业课程的一部分引入,但通过数字逻辑实验课程引入内容后,学生既可以理解基本组合逻辑和时序逻辑功能,也可以利用逻辑电路应用于工程实践。这种承前启后的实验课程内容,既简单易实现,又依托于工程实践,促进学生更好地理解 and 掌握理论知识,提升学生学习兴趣和学习的满足感,也为后续基础和专业课程均打下基础。

1 安全加密算法原理

安全密码技术自古以来被人们沿用,在电子、通信、计算机发展的时代^[6],加密算法作为信息安全保障的核心技术被广泛应用。在密码体制中有两种类型:对称密码体制和非对称密码体制,对应的算法为对称和非对称加密算法。这些安全算法可有效地保密信息安全、防止信息篡改和确认身份。20 世纪 70 年代美国公开的 DES 加密算法是应用最广的对称加密算法之一,其特点是算法的加密和解密过程使用相同密钥且保密。算法模型框图如图 1 所示。

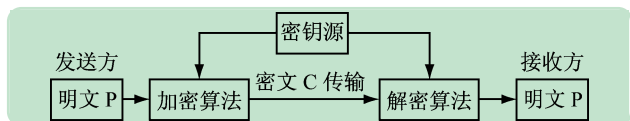


图 1 对称加密模型框图

图 1 中明文 P 通过加密算法加密后得到密文 C,传输给接收方,接收到的密文通过相同的安全密钥进行解密操作,得到发送方给予的信息内容。其中双方必须以安全通道获取密钥源,保障信息安全。而破译者只能在传输过程中获取密文,进行破译得到明文和密钥。

S-DES 是具有扩展性适用于教学的一种加密算法,由 Santa Clara 大学的 Edward Schaefer 教授提出^[7]。与 DES 加密算法基本原理基本相同且简单易实现,其内部核心部件采用 Feistel 结构,常被应用于

图像处理方面。S-DES 加密算法仍属于对称加密算法,在输入明文后经过 IP 置换、 F_k 函数、SW 交换、 IP^{-1} 逆置换进行加密运算得到密文 C,在此过程中密钥源形成子密钥,添加入 F_k 函数中。而接收方得到密文后同样采用该算法以相同方式进行运算,但区别于加密过程中子密钥的加载到 F_k 函数顺序完全倒置。S-DES 加密算法流程图如图 2 所示。

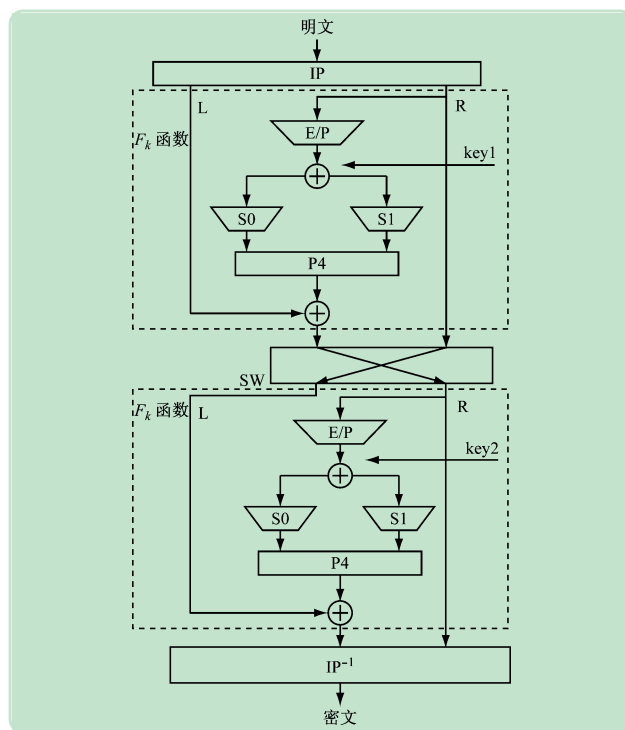


图 2 S-DES 加密算法流程图

图 2 中, L 和 R 代表数据的左、右部分各 4 bit, \oplus 代表异或操作。IP 置换是简单的数据位置互换,按照指定规则将原有 P1, P2, P3, P4, P5, P6, P7, P8 位置变换成 P2, P6, P3, P1, P4, P8, P5, P7; 与之相对应的 IP^{-1} 逆置换则将得到的数据变换为 D4, D1, D3, D5, D7, D2, D8, D6。主体运算为 F_k 函数,基本函数为

$$f_k(L, R) = (L \oplus F(R, SK), R) \quad (1)$$

式(1)中, L 和 R 表示数据左右两部分, SK 是子密钥之一, 而 \oplus 是逐位异或函数, F 为其内部 S-BOX 与置换操作。其内部包括扩展置换 E/P (左/右移位)、基于 Feistel 结构的 S-BOX 和循环左移操作,同时,扩展置换 E/P 后引入子密钥,与原数据异或操作,得到数据根据矩阵行列式位置选择 S-BOX 内部数据,组合得到运算结果。一轮运算后对调数据左右两部分,再次进行 F_k 函数的轮运算。最后一轮运算后直接将数据组合进行 IP^{-1} 逆置换得到密文 C。

图 2 中 key1 和 key2 表示右密钥源生成的两个子密钥。子密钥生成过程主要是左移运算,但移位数据有所不同。密钥源同样进行规定的置换操作,置换后数据分为左右两部分,分别左移 1 位,将其组合提取其

中 8 bit,即为子密钥 key1。同时上述数据组合后再左移 1 位,重新组合提取其中 8 bit,即为子密钥 key2。

2 安全加密系统仿真实验平台实现

根据加密算法原理逻辑性强运算流水性特点,本文利用 EDA 技术中 Quartus II 开发平台进行系统设计,同时借助 Visual C++ 仿真平台进行安全系统设计结果对比验证。该平台的图形化设计清晰形象,灵活性强、运算速度快,仿真验证效果直观,学生在有限的学时里可快速建立模型,验证正确性,激活了学生兴趣,提升学习效率和工程实践意识。

2.1 Quartus II 仿真实现

根据 S-DES 加密算法工作原理分析,算法加密与解密操作简单,硬件实现快速安全、灵活性较高^[8]。利用 Quartus II 平台可建立图形化模型,有利于学生分析和建模。系统结构图如图 3 所示。

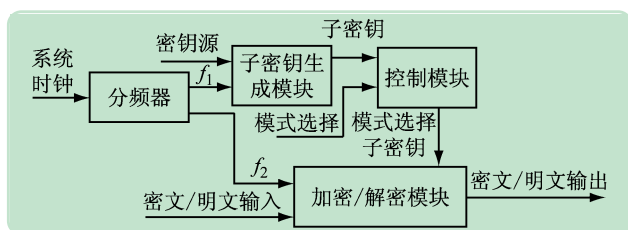


图 3 S-DES 系统设计结构图

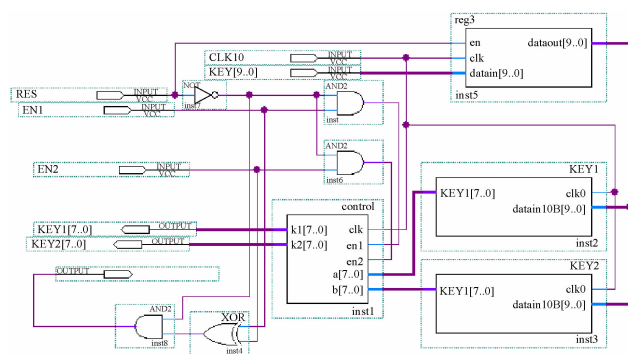
系统时钟加载入系统中,为保证系统运行稳定,对子密钥生成模块输入相对于加密/解密模块具有较高的频率,提前运行子密钥生成模块,为加密/解密模块运行做充分准备。控制模块可利用使能键进行加密和解密操作,最终输出正确结果。

Quartus II 是由 Altera 公司开发的一种综合性 FPGA/PLD 集成仿真工具软件^[9-10]。该平台支持多种硬件描述语言:VHDL、AHDL、Verilog HDL 等,用户可以利用 Quartus II 软件的文本输入方式、模块输入方式、EDA 设计输入工具等方式等进行电路描述。软件内部支持 IP 核,方便调用各种成熟模块,同时具有集成仿真工具。具有功能集成度高、界面统一、灵活性强、速度快等优点。

根据算法原理和系统结构,本文对结构图 3 中各个模块分别进行图形化设计,其各部分电路利用 Quartus II 平台内部模块调用及硬件语言编辑合成模块进行搭建。依据实验室内现有开发硬件平台具有 20 MHz 时钟晶振,设定系统时钟为 20 MHz,在系统内部高性能嵌入式模拟锁相环及 VHDL 语言编辑下进行分频操作,得到相差 10 倍的频率 f_1 和 f_2 分别输入至子密钥生成模块和加密/解密模块。

加密算法中由密钥源生成子密钥的过程及其重要,子密钥为主体运算提供钥匙,保证系统安全^[11-12]。

子密钥及控制设计电路图如图 4 所示。



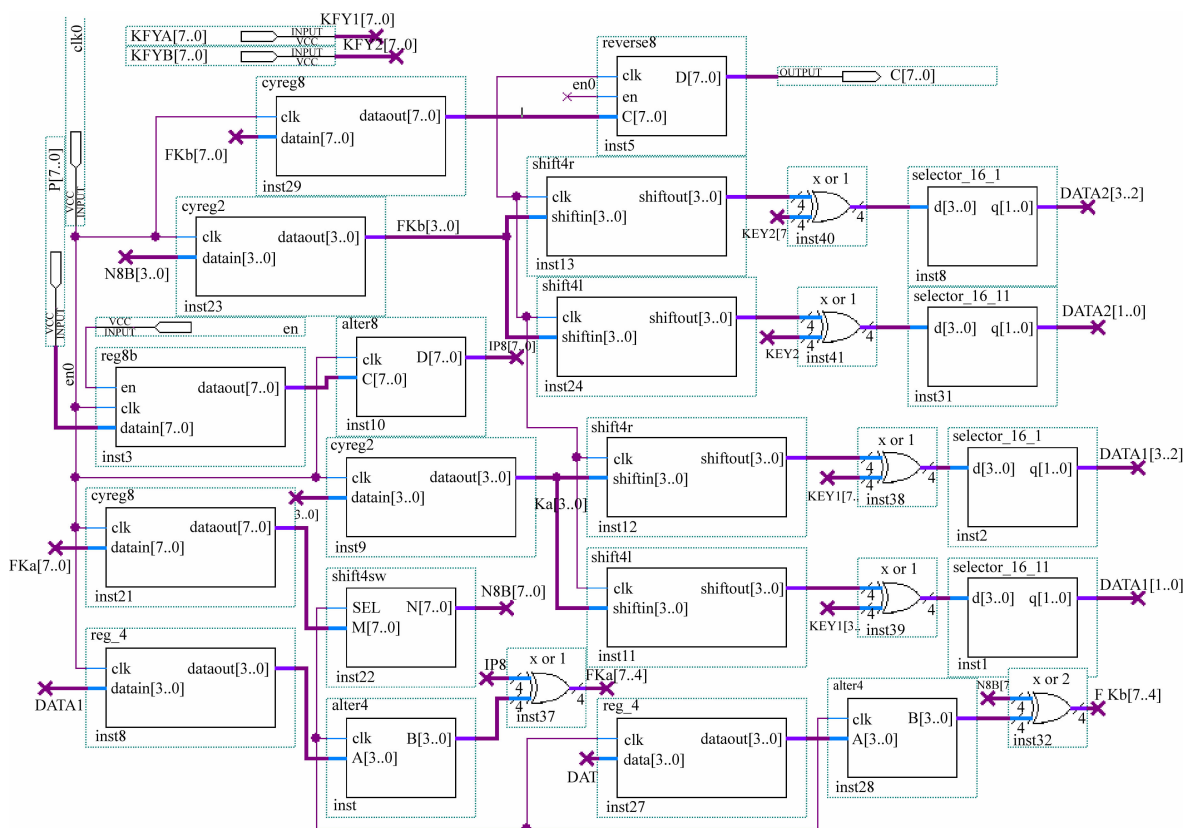


图5 加密/解密运算顶层设计电路图

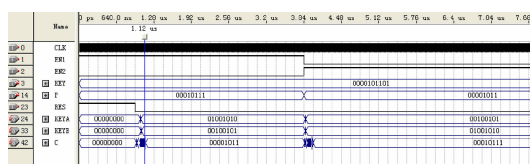


图6 S-DES 安全加密算法系统仿真图

证,提升对知识点的理解和学习兴趣。

界面工作区定义明文、密文、密钥源以及运算中间变量,根据 S-DES 工作原理对代码输入、密钥源输入、子密钥生成、 F_k 函数、异或操作、 IP 和 IP^{-1} 变换以及扩展置换等分别定义编辑,该算法的核心部分就是 F_k 函数,其内部具有非线性 S-BOX,可有效保证信息安全。 F_k 函数运算^[14]的主要程序如下:

```
Void fk( char sub_key[ 8 ])
{ int i;
  for(i = 0; i < 4; i++)
  { l[i] = code[i]; r[i] = code[i + 4]; } //分离数据
  for(i = 0; i < 8; i++)
  temp[i] = XOR(r[ EP[i] - 1 ], sub_key[i]);
  //扩展后异或操作
  for(i = 0; i < 4; i++)
  { ln[i] = temp[i]; rn[i] = temp[i + 4]; }
  //左右数据分别存放
  box(ln, S_a); // S-BOX0 运算
  temp[4] = temp[6];
  temp[5] = temp[7]; //移位置
  box(rn, S_b); // S-BOX1 运算
```

```
temp[0] = temp[5]; temp[1] = temp[7];
temp[2] = temp[6]; temp[3] = temp[4];
//P4 置换
for(i = 0; i < 4; i++)
l[i] = XOR(temp[i], l[i]); i = 0;
//左右数据再次异或
while(i < 4) { code[i] = l[i]; i++; }
while(i < 8) { code[i] = r[i - 4]; i++; } //合并数据
```

通过程序编写,编译成功后运行程序,得到界面如图7所示。

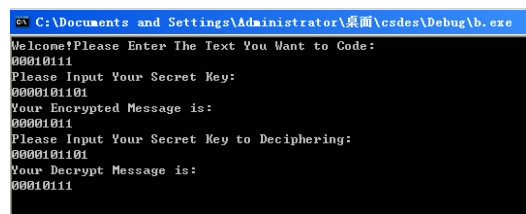


图7 Visual C++ 加密系统仿真

通过 Visual C++ 平台系统仿真,可以观察到基于软件实现的 S-DES 加密算法运算过程中明文、密钥源及密文与硬件编辑开发平台 Quartus II 输入相同的情况下,系统仿真结果完全相同。在图形化设计与语言编辑设计两种方式实现过程中,学生可充分理解时序逻辑电路与组合逻辑电路的系统功能,同时,以工程角度在多种设计形式下,增强学生对知识应用的灵活性。

(下转第 161 页)

题,有效提高了实物实验的教学效果。同时,也为慕课课程的实验教学和实验管理提出了一体化解决思路。

从涵盖实验原始数据的实验报告模板的自动生成,到实验报告的在线完成和网上提交,以及实验报告的自动批改,实现了实验报告的无纸化。也为实验教学数据规范化管理,建立历史实验数据库查询等衍生功能创造了条件。

参考文献(References):

- [1] 邹广平,夏兴有. 力学实验教学改革研究与实践[J]. 黑龙江教育(理论与实践),2015(3):65-66.
- [2] 苏 辛. 慕课来了[J]. 中国远程教育,2013(13):1-3.
- [3] 李 斐,黄明东. “慕课”带给高校的机遇与挑战[J]. 中国高等教育,2014(7):22-26.
- [4] 斯蒂芬·哈格德[英],慕课正在成熟[J]. 王保华,何欣蕾(译). 教育研究,2014,35(5):92-99.
- [5] 徐光涛. 慕课本土化需要创新[J]. 上海教育,2013(31):8-9.
- [6] 张 颖,王艳芳. 互动式网络实验教学综合平台建设[J]. 实验室研究与探索,2014,33(9):162-165.
- [7] 武晓峰,高晓杰. 高校实验室建设发展报告(2014 中国高等教育学会实验管理工作分会系列专题报告)[M]. 北京:清华大学出版社,2014.
- [8] 胡 征. 现代实验室建设与管理指南[M]. 天津:天津科技翻译出版公司,2014.
- [9] Satheesh Mithun. Web Development with MongoDB and NodeJS[M]. Newyork:Packt Publishing, 2015.
- [10] Green Brad, Seshadri Shyam. 用 AngularJS 开发下一代 Web 应用[M]. 大漠穷秋译. 北京:电子工业出版社,2013.
- [11] Dayley Brad. Node.js + MongoDB + AngularJS Web 开发[M]. 卢涛,李 颖译. 北京:电子工业出版社,2015.
- [12] [美]Nicholas C Zakas. 高性能 JavaScript[M]. 丁琛译. 北京:电子工业出版社,2015.
- [13] [美]劳里亚特著. 深入 Ajax: 架构与实践[M]. 张过等译. 北京:人民邮电出版社,2009.
- [14] [美]Chun Wesley J, Python 核心编程[M]. 2 版. 北京:人民邮电出版社,2008.
- [15] [美]施瓦茨(Schwartz B)等,高性能 MySQL[M]. 3 版. 宁海元,周振兴等译. 北京:电子工业出版社,2013.

(上接第 109 页)

3 结 语

基于计算机专业数字逻辑课程培养方向和目标,以安全加密算法中 S-DES 算法原理为基础,利用 Quartus II 平台进行图形化设计以及在 Visual C++ 平台上的 C 程序化设计分别实现该算法,多种形式下进行系统仿真,对比实验结果验证其准确性。设计内容承上启下,难度适中,灵活性强且可扩展至其他复杂的加密算法,既有助于数字逻辑课程内容理解,也为后续计算机组成原理、微机原理、云计算等课程打下良好知识基础。该实验平台拓展学生数字系统设计思维,提升了学生工程实践意识,也增强了课程学习兴趣。

参考文献(References):

- [1] 田淑珍,贾玉荣. 仿真工具在数字逻辑实验中的应用[J]. 实验技术与管理,2015,32(1):124-126.
- [2] 李 文,黄 文,赵全友,等. Multisim 仿真的数字逻辑工程素养培养[J]. 实验室研究与探索,2014,33(12):62-65.
- [3] 盛建伦,巩玉玺,刘淑霞,等. 计算机专业硬件基础课程实验教学体系的研究[J]. 实验室研究与探索,2013,32(10):387-391.
- [4] 盛建伦,刘淑霞,王 勇,等. 数字逻辑实验技术改革的研究[J]. 实验技术与管理,2015,32(4):216-219.
- [5] 唐志强. 计算机专业数字逻辑实验的改革与创新[J]. 实验室研究与探索,2013,32(10):182-184.
- [6] 郑 东,赵庆兰,张应辉. 密码学综述[J]. 西安邮电大学学报,2013,18(6):1-10.
- [7] William Stallings 著. 杨 明等译. 密码编码学与网络安全:原理与实践[M]. 3 版,北京:电子工业出版社,2001:181-187.
- [8] Tselepis I N, Bekakos M P. An FPGA hardware parallel implementation of the DES algorithm[J]. Neural Parallel and Scientific Computations,2004,12(4):1061-5369.
- [9] 刘若鹏. 电子式互感器数据采集器的研究[D]. 成都:西华大学,2013:31-33.
- [10] 王振华. 基于 FPGA 的超高速数据采集系统的开发[D]. 北京:清华大学,2006:90-99.
- [11] 黄 慧,江荣荣,谭 敏,等. 基于 FPGA 的加密算法实现[J]. 合肥学院学报(自然科学版),2015,25(1):35-38.
- [12] 付 莉. 一种基于改进 DES 算法的高效率 FPGA 硬件实现[J]. 桂林电子科技大学学报,2009,29(6):493-496.
- [13] 易 艺,郝建卫. FPGA 在数字逻辑电路教学中的应用[J]. 实验科学与技术,2016,14(2):12-15.
- [14] 郝 伟,曹代勇,胥 哲,等. 中国煤炭特性数据库数据加密技术研究[J]. 中国煤炭,2008,34(10):58-60.

· 名人名言 ·

建立以提高教育质量为导向的管理制度和工作机制,把教育资源配置和学校工作重点集中到强化教学环节、提高教育质量上来。制定教育质量国家标准,建立健全教育质量保障体系。加强教师队伍建设,提高教师整体素质。

——摘自《国家中长期教育改革和发展规划纲要》