DES 算法原理及其 FPGA 实现

解双建,原 亮,谢方方
(军械工程学院 计算机工程系,河北 石家庄 050003)

摘 要:DES(数据加密标准)是最常用的加密算法之一,自诞生至今一直被广泛应用于各个行业领域。为了深刻理解 DES 算法的运算过程和实现方法,在详细讨论 F 函数和 S 盒这两个关键因素的基础上,利用 Xilinx 公司的综合开发工具 ISE 和 Spartan3E FPGA 等工具,设计了 FPGA 与 PC 机的串口通讯,完成了 DES 算法在 FPGA 中的正确实现,并采用软件仿真和硬件实现得出了实验结果,给出了 DES 算法在 FPGA 中的资源利用情况。通过实验结果和资源利用率验证了 DES 算法的功能及其在低端 FPGA 上的实用性。

关键词:DES 算法; S 盒; 硬件实现; FPGA
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)07-0158-03

The Principle of DES Algorithm and Realization on FPGA

XIE Shuang-jian, YUAN Liang, XIE Fang-fang
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: DES(data encryption standard) is one of the most popular encryption algorithms and has been widely used in many fields since its appearance. Based on the discussion of the two key factors of F-function and S-box, the principle and the process of DES is introduced in detail. The communication between FPGA and PC is designed and the correct realization of DES is completed on Spartan3E FPGA by implementing ISE tools. Not only the results of simulation on software and experiment on FPGA but also the inner source utilization are presented, which explain the function of DES and its adaption to low-grade FPGA.

Key words: DES algorithm; S-box; hardware realization; FPGA

0 引 言

随着计算机和通信技术的快速发展,大量电子数据相应产生。在人们对电子信息越发依赖的同时,数据安全问题也日益突出[1]。尤其是在军事、金融领域,甚至是一般的政府部门,信息的保护工作显得格外重要。1973 年,美国国家标准局开始研究除国防部外的其它部门的计算机系统的数据加密标准,先后两次向公众发出了征求加密算法的公告。1977 年初,美国政府采纳了 IBM 公司设计的 DES 方案作为非机密数据的正式数据加密标准。

DES 加密算法不仅实现了加密算法的国际标准化,而且满足了设计之初的四点要求[2]:

(1) 提供高质量的数据保护,防止数据未经授权的泄露和未被察觉的修改;

(2) 具有相当高的复杂性,要使破译的开销超过可能获得的利益,同时又要便于理解和掌握;

(3) 算法的安全性只依赖于密钥,而不是算法本身,其安全性仅以密钥为基础;

(4) 易于实现,运行有效,并且适用于多种完全不同的应用领域。

DES 算法的安全性在于其密钥的安全性,而算法本身是公开的。DES 是一种最通用的迭代型对称密钥算法,属于分组密码算法[3]。对称算法的对称性体现在加密密钥能够从解密密钥推算出来,反之亦然。在大多数对称算法中,加解密的密钥是相同的。

1 DES 加密算法原理

DES 算法的入口参数有: Key、Data、Mode。Key 为 8 个字节共 64 位,是 DES 算法的工作密钥; Data 也为 8 个字节 64 位,是要被加密或被解密的数据; Mode 为 DES 的工作方式,有两种: 加密或解密。由于 DES 算法是一种高度对称算法,其解密过程仅为加密过程的逆运算,因此,文中只讨论 DES 算法的加密模式。

1.1 DES 运算过程

DES 加密算法是将 64 位的明文输入块变为 64 位

收稿日期:2010-12-18; 修回日期:2011-03-21
基金项目:国防科技重点实验室基金项目(9140C8702020803)
作者简介:解双建(1986-),男,硕士研究生,研究方向为计算机体系结构; 原 亮,教授,硕士生导师,研究方向为计算机体系结构、电磁仿生理论与实现。

的密文输出块。其密钥是 64 位,其中每个密钥字节的最后一位是奇偶校验位,故有效的密钥长度为 56 位。DES 的整体结构采用 16 轮 Feistel 模型[4,5],其加密过程如图 1 所示。待加密的 64 位明文数据首先进行初始变换 IP,然后将置换后的 64 位数据分为左半部分 L_0 和右半部分 R_0 各 32 位,接着进行 16 轮迭代。在每一轮中,右半部分在 48 位子密钥 k 的作用下进行 f 变换,得到的 32 位数据与左半部分按位异或,产生的 32 位数据作为下一轮迭代的右半部分,原右半部分直接作为下一轮迭代的左半部分,但第 16 轮(最后一轮)不进行左右互换。其轮函数的数学描述为:

$$L_i = R_{i-1}, R_i = L_{i-1} \oplus f(R_{i-1}, k_i), i = 1,2,\cdots,16$$

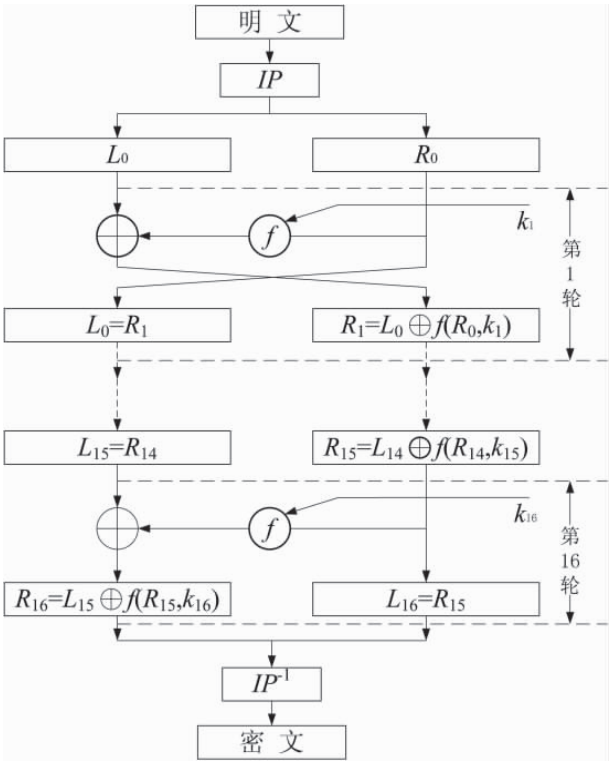

图 1　DES 加密运算过程

其中 $k_i(i = 1,2,\cdots,16)$ 为第 i 轮的子密钥,L_i 和 $R_i(i = 1,2,\cdots,15)$ 分别为第 i 轮迭代后输出的左半部分和右半部分,R_{16} 和 L_{16} 为第 16 轮迭代后输出的左半部分和右半部分,最后对 64 位的 (R_{16}, L_{16}) 进行末置变换 IP^{-1},所得结果即为密文。

初始变换 IP 只是按照特定的置换表对 64 位明文数据的结构作初步的调整; 末置变换 IP^{-1} 是初始变换的逆运算,是对 16 轮迭代后的结果按照特定的置换表进行移位运算。初始变换和末置变换用以打乱 64 位数据的 ASCII 码字划分的关系,其密码意义不大,对 DES 的安全性不起本质作用[6]。

1.2　F 函数

F 函数是 DES 算法的核心。从图 1 可以看出,F 函数有两个输入,一个是轮输入右半部分的 32 位数据 R,另一个是由初始密钥通过密钥生成算法产生的 48 位子密钥 k。F 函数的运算过程如图 2 所示,不妨设 $R = a_1a_2\cdots a_{32}$,$k = k_1k_2\cdots k_{48}$,即得:

$$f(R,k) = P(S(E(R) \oplus k))$$

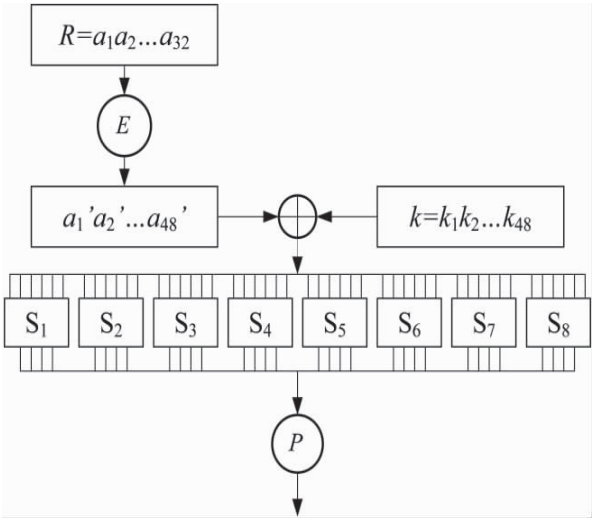

图 2　F 函数

(1) 扩展变换 E 的作用是将输入的 32 位数据扩展为 48 位,具体扩展方法是首先将 32 位数据分成 8 个 4 位块,然后将每个 4 位块扩展成 6 位块。具体地说,是将一个 4 位块的左相邻位和右相邻位分别放到该块的左侧和右侧,从而形成一个 6 位块。

(2) S 盒是将 48 位输入转化为 32 位数据输出,S 盒共有 8 个,每个 S 盒都是将 6 位输入转化为 4 位输出。具体来讲,E 盒扩展后的 48 位数据与子密钥 k 按位异或,然后将得到的 48 位数据从左到右分成 8 个 6 位,分别作为 8 个 S 盒的输入,对于每个 S 盒,将 6 位输入的左右两位对应的十进制数作为相应的行,中间四位对应的十进制数作为相应的列,然后在每个 S 盒各自的变换表[7] 中查找相应的十进制数,最后将其转化为相应的 4 位二进制数即为该 S 盒的输出。

(3) P 盒是在特定的置换表下将 S 盒输出的 32 位数据移位变换后作为 F 函数的最终结果输出。

1.3　S 盒的设计特点

S 盒变换是 DES 算法中唯一的非线性变换,其密码学性质的好坏对 DES 的安全性起着至关重要的作用。人们对 DES 的 S 盒进行了广泛而深入的研究,总结出一些设计特点[8] 如下:

(1) 每个 S 盒的每一行都是 0 到 15 的一个置换;

(2) 每个 S 盒的每一位输出都不是输入的线性或仿射函数;

(3) S 盒输入变化一位,输出变化至少两位;

(4) 对任意的 S 盒和任意 6 位二进制输入 $x(x \in \{0,1\}^6)$,$s(x)$ 和 $s(x \oplus 001100)$ 至少有两位不同;

(5) 对任意的 S 盒和任意 6 位二进制输入 x,以及

任意的 $a,b \in \{0,1\}$，都有 $s(x) \neq s(x \oplus 001100)$；

(6) 对任意的 S 盒，当它的输入位中某一位固定，其他五位变化时，所有输出数字中 0 和 1 的总数接近相等。

随着人们对 S 盒的不断深入了解，有关 S 盒的设计问题便成了人们争论的焦点[9,10]。美国国家安全局曾修改过 S 盒，但没有说明修改的原因。现用的 S 盒都是修改之后的，其结构也是固定的，它的设计原则从未完全公开。所有这些足以让人们怀疑 S 盒中可能嵌入了陷门，倘若真是如此，了解陷门的人就能成功地获取密码并进行分析。

2 FPGA 实现过程

采用 FPGA(Field Programmable Gate Arrow，现场可编程门阵列) 实现具有开发周期短、开发成本低等优点，并且易于同其他模块的综合验证[11]。为适合于成本较小的低端应用领域，同时能保证一般网络通信的运算速度，文中采用了 Xilinx 公司的 Spartan - 3E XC3S500E 型[12] FPGA 作为算法的硬件实现载体。

2.1 FPGA 硬件结构

系统以 RS232 作为数据传输通道，采用 USB 下载模式下载至 PROM(支持掉电不丢失) 和 FPGA 芯片中，通过串口调试工具向 FPGA 收发明文和密文来进行 DES 算法的硬件实现，其系统结构如图 3 所示。

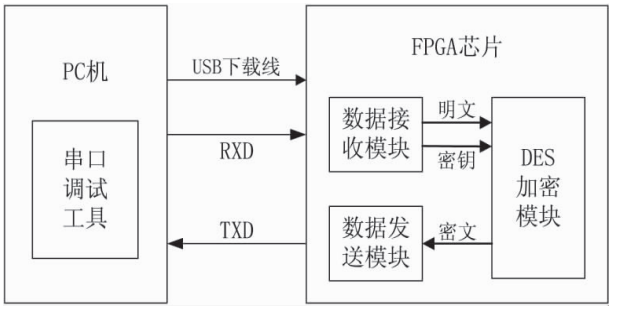

图 3 系统结构图

DES 加密程序由数据接收模块、加密模块和数据发送模块构成。数据接收模块是将串口调试工具发送的 128 位串行明文和密钥数据转化为并行数据；加密模块把明文加密后的密文以 64 位并行数据输出；数据发送模块是把 64 位并行密文数据转化为串行数据发回给串口调试工具。

2.2 功能验证

实验对 DES 算法的加密和解密功能都进行了仿真，仿真实验结果如图 4 所示。图中左侧：clk 为时钟信号，ikey 为密钥，imsg 为输入数据，odata 为输出数据，dec 为加解密控制信号。仿真过程中，加密和解密共用同一密钥 FF00FF00FF00FF00(HEX)，对明文 00FF00FF00FF00FF(HEX) 进行加密后所得密文为 8234C3738EE42FBD(HEX)，相反之，对于密文 8234C3738EE42FBD(HEX) 进行解密可得明文 00FF00FF00FF00FF(HEX)。

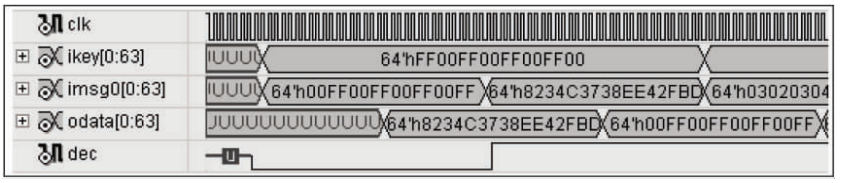

图 4 仿真结果

硬件实验只对 DES 算法的加密功能进行实现，其结果如图 5 所示。系统借助串口调试工具向 FPGA 发送数据 EB9000FF00FF00FF00FFFF00FF00FF00FF00(HEX)，接收到的密文为 8234C3738EE42FBD(HEX)。发送数据中明文为 00FF00FF00FF00FF(HEX)，密钥为 FFF00FF00FF00FF00(HEX)，EB90 为数据头，是数据在接收模块和发送模块中的标识符。

图 5 硬件实现结果

软件仿真和硬件实现的结果验证了实验的正确性，同时也验证了 DES 算法的功能。

2.3 性能分析

系统用 Verilog HDL 语言实现，以 Xilinx ISE 作为综合工具，ISE Simulator 作为仿真软件，对 DES 进行了综合仿真，得到的仿真报告内容如表 1 所示。

表 1 仿真报告表

Target Device:	xc3s500e - 4fg320	
Number of occupied Slices	2,116 out of 4,656	45%
Number of Slice Flip Flops	1,264 out of 9,312	13%
Number of 4 input LUTs	3,416 out of 9,312	36%
Number of bonded IOBs	4 out of 232	2%
Number of DCMs	1 out of 4	25%

从综合仿真报告中可以看出，实验占用了较少的硬件资源。DES 算法对硬件要求较低，不仅节约了应用成本，且进一步推动了 DES 算法的广泛应用。

3 结束语

文中详细讲述了DES算法的运算过程和内部结

(下转第 164 页)

接口函数(见表 1) 。

5 性能测试

在 Linux2. 4 内核下,采用手动配置 IPSec 密钥的方式,在 ESP 隧道模式下利用两网关互 ping 的方式[11]进行 IPSec 加密卡的性能测试,并使用 ethereal 进行网关间抓包[12]对数据进行加解密及散列分析(测试结果见表 2) 。

表 2 网关互 ping 测试结果

处理形式	吞吐率(/Mbps)	数据安全性
AES + MD5	38. 147	数据流保密
AES + SHA1	36. 235	数据流保密

对加密卡性能进行单独测试,主要性能参数是实现加解密及认证的速率,结果见表 3。

表 3 加密卡性能测试结果

处理方式	吞吐率(/Mbps)	时钟频率(MHz)
AES(ECB)	549. 868	98. 8
AES(CBC)	477. 434	93. 25
HMAC – SHA1	293	47. 51
HMAC – MD5	253	33. 62

实验结果表明,硬件实现 IPSec 协议都可以保证数据的高速安全传输,完全满足高速网络的需求。

6 结束语

IPSec 协议对于保证虚拟专用网的网络安全性具有极其重要的意义。文中实现了基于开源 Linux 操作系统的 IPSec 硬件加速,适用于 VPN 数据安全传输; 采用软硬件结合的方式,极大地缩短了开发周期,而完善的接口函数允许用户在此基础上进行二次开发,具有高安全性、高速及可扩展性等优点。

参考文献:

[1] 蔡集明,陈 林. 对 IPSec 中 AH 和 ESP 协议的分析与建议[J]. 计算机技术与发展,2009,19(11) : 15 – 17.

[2] RFC2401: Security Architecture for the Internet Protocol [S]. 1998.

[3] Kent S, Atkinson R. RFC 2401 Security Architecture for the Internet Protocol [S]. 1998.

[4] 罗恒洋. IPSec 在 MPLS VPN 中的应用 [J]. 计算机技术与发展,2009,19(3) : 168 – 171.

[5] 孙 黎. IPSec 安全芯片的设计与实现 [D]. 西安: 西北工业大学,2007.

[6] Hamed H. Modeling and verification of IPSec and VPN security policies [C] //13th IEEE International Conference. [s. l.]: [s. n.],2005.

[7] 林建德. 北京: 中国 VPN 市场研究年度报告 [R]. 北京: [出版者不详],2005.

[8] 高振栋. 动态 IP 环境下 IKEv2 扩展设计与改进 [J]. 计算机技术与发展,2008,18(12) : 162 – 165.

[9] Wilson C, Peter D. 虚拟专用网的创建与实现 [M]. 北京: 机械工业出版社, 2000.

[10] Rubini, Jonathan. linux 设备驱动程序 [M]. 魏永明, 译. 北京: 中国电力出版社, 2002.

[11] 杨黎斌,慕德俊,蔡晓妍,等,基于硬件加密的嵌入式 VPN 网关的实现 [J]. 计算机工程与应用,2007,43(4) : 122 – 125.

[12] 顾文婷,潘雪增,楼学庆,等,面向 IPsec 安全策略的 VPN 性能评估模型 [J]. 计算机工程与应用,2009,45(36) : 78 – 81.

(上接第 160 页)

构,在低成本 FPGA 上成功实现了 DES 算法的功能。通过综合仿真和硬件实现验证了算法的正确性和实用性。

参考文献:

[1] 刘 涛,胡佳伟. 校园网络环境下数据加密的研究与设计[J]. 计算机技术与发展,2008,18(1) : 171 – 174.

[2] 王衍波,薛 通. 应用密码学 [M]. 北京: 机械工业出版社,2003.

[3] 普运伟,耿植林,楼 静. 从 DES 算法论分组密码的设计原则 [J]. 微机发展(现更名: 计算机技术与发展) ,2005,15(5) : 57 – 59.

[4] Lagger A. Implementation of DES Algorithm Using FPGA Technology [R]. [s. l.]. Microelectronic Systems Laboratory Winter Semester Project, 2002.

[5] 金晨辉,郑浩然,张少武,等. 密码学 [M]. 北京: 高等教育出版社,2009.

[6] Drimer S. Security for Volatile FPGAs [D]. London: Philosophy to the University of Cambridge, Darwin College,2009.

[7] Kahate A. 密码学与网络安全 [M]. 邱 仲,译. 北京: 清华大学出版社,2005.

[8] 陈雪林,王 毅. DES 算法的 S 盒分析 [J]. 内肛科技,2007,8(7) : 139 – 140.

[9] 曹建国,王 丹,王 威. 基于 RSA 公钥密码安全性的研究 [J]. 计算机技术与发展,2007,17(1) : 172 – 173.

[10] Raphael C. Reducing the exhaustive key search of the data encryption standard [R]. Malaysia: Information Security Research Lab, Swinburne University of Technology,2006.

[11] 张春辉. DES 算法原理及改进 [J]. 电脑知识与技术,2009,5(22) : 6173 – 6174.

[12] 李 辉. 基于 FPGA 的数字系统设计 [M]. 西安: 西安电子科技大学出版社,2008.