

一种高速高安全性的 DES 算法设计

温 泉¹, 赵红敏², 郝晓东², 沈海鸿¹

(1 中国地质大学(北京) 信息工程学院, 北京 100083;

2 大唐微电子有限公司, 北京 100094)

摘 要: 在详细分析 DES 算法设计原理基础上, 针对 DES 算法的运算速度和安全性进行综合考量, 提出一种高速高安全性的 DES 算法设计. 将算法执行速度提高了四倍, 通过运算时钟随机化同步增强了算法的安全属性. 最后通过对 DES 算法模块设计结果进行仿真验证及综合, 表明此设计达到了性能和面积的综合优化, 满足了加密 IP 应用领域对速度和安全性日益提高的需求.

关键词: DES 算法; Verilog; 高速; 高安全性; 时钟随机化

中图分类号: TN47

文献标识码: A

文章编号: 1000-7180(2014)12-0164-04

A High-speed and High Security DES Algorithm Design

WEN Quan¹, ZHAO Hong-min², HAO Xiao-dong², SHEN Hai-hong¹

(1 School of Information Engineering, China University of Geosciences (Beijing), Beijing 100083, China;

2 Datang Microelectronics Technology Co., LTD, Beijing 100094, China)

Abstract: Based on the theory of DES algorithm, the present study improves DES algorithm hardware design in the way of operation speed and security. The optimized design increases the executive speed of DES algorithm by 4 times, and enhances the security of algorithm by adding a module of optional random clock. Simulation verification and synthesize are implemented on DES algorithm Verilog design. Optimized design achieve integrated consideration between chip area and performance, to realize high-speed and high security DES algorithm, satisfying advanced requirements of speed and security in the field of encryption IP core application.

Key words: DES algorithm; verilog; high-speed; high security; random clock

1 引言

数据加密标准(Data Encryption Standard, DES)是一种使用密钥对明文或密文进行加解密的分组数据加密算法, 1976 年被美国联邦政府的国家标准局确定为联邦资料处理标准, 至今仍作为安全算法被广泛应用^[1]. 目前在国内, DES 算法在 POS、ATM、磁卡及智能卡(IC 卡)、加油卡、高速公路收费卡等方面已实现了关键数据的保密.

本文通过对 DES 算法的原理分析, 将标准的 16 轮循环迭代完成一次加解密运算改进为只需要 4 轮循环迭代即可完成, 大大提高了算法执行速度. 此

外, 由于加解密运算时容易被外部通过功耗分析技术而恶意攻击, 本文在算法模块设计中加入时钟随机化设计, 保证了运算时模块功耗的不确定性, 有效保护密钥及明文, 从而增强 DES 算法的安全属性. 最终实现了高速高安全性的改进型 DES 算法设计.

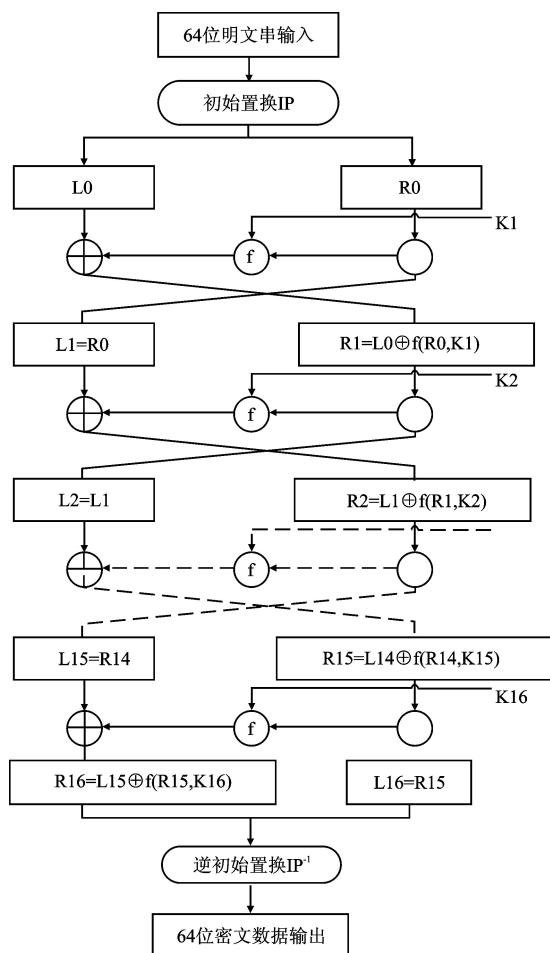
2 DES 算法

DES 是一个分组加密算法, 其基本思想是用一个 56 比特的密钥来加密一个 64 比特的明文串, 输出一个 64 比特的密文串. 其中, 使用密钥为 64 比特, 实用 56 比特, 另外 8 位用作奇偶校验. 加密的过程是先对 64 位明文分组进行初始置换, 在左、右两

收稿日期: 2014-03-01; 修回日期: 2014-04-21

基金项目: 中国地质大学(北京)基本科研业务费专项基金

部分分别经过 16 轮迭代后,再进行循环移位与变换,最后进行逆变换得出密文^[2-3].如图 1 为 DES 算法流程图.



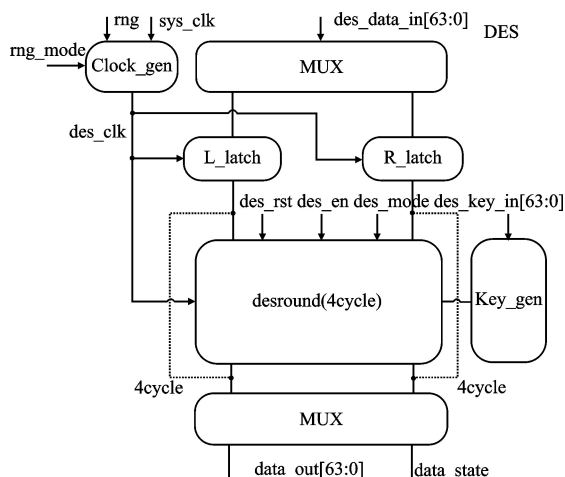


图2 DES算法硬件设计框图

思路是从16轮加解密迭代过程着手,以往一个周期完成一轮加解密迭代,DES算法通过不同的变换来实现数据的加解密,使用组合逻辑实现轮运算,这就为减少DES算法的执行周期提供了可能。

本设计用空间换速度的方法,将一组轮迭代单元增加至4个,可实现一个周期内完成4轮加密迭代,这样16轮运算只需4个时钟周期即可完成,加上数据输入输出使能,一次DES加解密运算只需6个时钟周期。

4轮迭代单元构成一个desround核,一个时钟内数据通过desround核可完成4次迭代运算,16轮只需4个时钟。由于增加了三组轮迭代单元,设计比标准DES算法要增加数字逻辑,在华虹0.13 μm 工艺下进行了综合,面积结果为标准算法的1倍。但将DES运算时间缩减了2/3。本设计与全流水线结构的DES算法相比较节约了硬件代价,达到了速度与逻辑门数的综合平衡。

3.2 DES算法高安全性优化设计

DES算法主要由置换和扩散构成,易于用硬件实现。然而由于分组密码多次循环迭代的共性,在实现该算法的过程中硬件功耗呈现某种特征^[4],这使得攻击者可以通过收集芯片DES加解密过程的功耗曲线,并利用统计的方法对所收集到的曲线进行分析处理^[5],从而分析破解出DES算法密钥。这种方法被称为功耗分析技术,对信息安全构成了极大威胁。为了提高DES算法的安全性,设计中使用了随机数时钟模块clock_gen,如图2所示。其设计原理是将原运算时钟与输入的随机数(1 bit)做逻辑运算,得到有效时钟沿随机出现的DES时钟。采用这种方式用来完成DES加解密算法的时钟数是不定

的,可以有效掩盖功耗变化的特征。利用时钟频率的随机变化对算法芯片的功耗进行扰乱,攻击者若得到明显的功耗特征,应使所有功耗样本曲线中任意时间点上进行的操作保持一致,而加入时钟随机模块,使各时间点上所发生的操作不能真正对准,差分特征将无法显现,从而保护DES算法的运算过程,提高了算法的安全性^[6]。

设计中DES运算时钟是否随机化可通过rng_mode位做选择,在需要做防攻击保护时打开,而在需要DES高速运行期间可以选择关闭随机化,因此兼顾了高速和高安全的特点。

4 仿真实验及综合

在电路实现时用Verilog语言描述了DES算法模块设计,使用Modelsim SE6.2b和Debussy完成功能仿真验证,利用synopsys DC综合工具在华虹0.13 μm 1.8 V CMOS工艺库下对硬件模块进行逻辑综合和优化。图3所示为改进的DES算法模块仿真波形,图4所示为标准DES算法模块仿真波形,比较两图可看出高速DES算法只需6个时钟周期就完成一次加密,而标准DES算法设计需要18个时钟,高速DES算法设计大大提高了DES模块的运行速度。

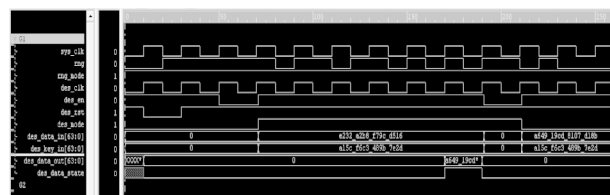


图3 DES算法高速设计仿真波形

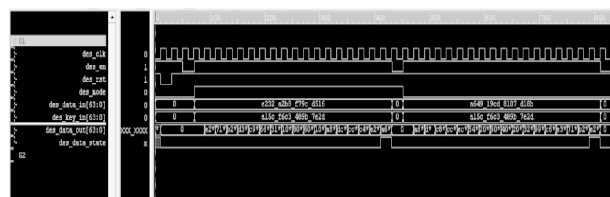


图4 DES算法16轮仿真波形

图5所示为选择使用随机时钟DES算法的仿真波形。图中DES算法的完成周期是不定长的,但需要满足6个时钟上升沿,使得每次完成DES算法加解密不具规律性,这种设计提高了DES算法的安全性。

从synopsys DC综合的结果看,改进的DES算法模块的面积是标准DES算法的2倍,而执行速度

比标准 DES 算法节约了 2/3 的时间,在 50 MHz 时钟频率下,改进的 DES 算法的处理性能可达到 533 Mb/s(表 1)。

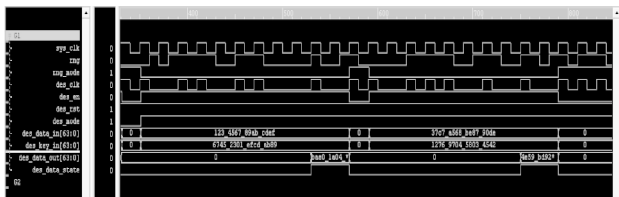


图 5 DES 算法使用随机时钟仿真波形

表 1 标准 DES 与改进 DES 算法面积与性能比较

	面积/ μm^2	处理性能/ (Mb/s)	加解密所需 时钟周期
标准 DES 算法	17 917	178	18
改进 DES 算法	36 151	533	6(最快)/Random

5 结束语

本文在 DES 算法基础上提出一种改进的 DES 算法设计,既优化了 DES 算法的执行速度又提高了算法的安全性。仿真及综合结果表明采用改进方法实现的 DES 算法满足深亚微米条件下集成电路设计对性能和面积的要求,适用于在速度与安全性都有较高要求的加密芯片应用领域。

参考文献:

- [1] 汪翼,沈海斌,何乐年,等. DES 算法的高速流水线实现[J]. 微电子学与计算机,2003,20(8):158-160.
- [2] Stinson DR. 密码学原理与实践[M]. 北京:电子工业出版社,2009.
- [3] Zodpe H D, Wani P W, Mehta R R. Design and implementation of algorithm for DES cryptanalysis[C] // 2012 12th International Conference on Hybrid Intelligent Systems (HIS). Pune: IEEE, 2012: 278-282.
- [4] 蒋惠萍,毛志刚. 一种抗差分功耗攻击的改进 DES 算法及其硬件实现[J]. 计算机学报,2004,27(3):334-338.
- [5] Li J, Lv Y X, Sun H F, et al. A power analysis resistant DES cryptographic algorithm and Its hardware design[C] // 2012 Third International Conference on Digital Manufacturing & Automation. GuiLin: IEEE, 2012: 121-124.
- [6] 李杰,单伟伟,吕宇翔,等. 一种抗相关功耗攻击 DES 算法及 FPGA 电路实现[J]. 东南大学学报:自然科学版,2012,42(6):1063-1068.

作者简介:

温泉 男,(1983-),硕士研究生.研究方向为数字集成电路设计,通信与网络技术. E-mail: wunquan@outlook.com.
沈海鸿 女,(1970-),博士,副教授,硕士生导师.研究方向为通信网络技术研究。

(上接第 163 页)

参考文献:

- [1] 斯蒂尔. 安全模式: J2EE、Web 服务和身份认证管理最佳实践和策略[M]. 北京:机械工业出版社,2006.
- [2] 马蕾,杨洪雪,朱青松. 基于改进身份认证协议的单点登录系统研究[J]. 微电子学与计算机,2012,29(7):182-183.
- [3] 王建雄. 网站注册与登录安全设计[J]. 大众科技,2010(4):11-12.
- [4] 郑爱媛. 在 JAAS 基础上的 Java 安全编程[J]. 电脑编程技巧与维护,2008(14):59-67.

- [5] 王敏,吉逸. Java2 环境下身份认证和授权机制的研究[J]. 微机发展,2003,13(5):40-42.
- [6] 刘晓华. 精通 Java 核心技术[M]. 北京:电子工业出版社,2003.

作者简介:

程俊波 男,(1964-),硕士,高级工程师.研究方向为计算机网络与信息安全研究. E-mail: cjbcs1@126.com.
肖瑜 男,(1964-),教授.研究方向为作战仿真与虚拟现实研究。