# 基于FPGA的DES掩码算法硬件设计与实现

王创伟,丁国良,尹文龙,常小龙
(军械工程学院 计算机工程系,河北 石家庄 050003)

**摘 要**:随着FPGA芯片在安全领域上的广泛应用,有关FPGA密码芯片的抗DPA研究也越来越受关注,但目前的研究成果大多针对智能卡的安全防护。针对功耗分析技术的特点及关键技术,特别是DPA技术进行研究,提出了具体的改进防御方法。使用硬件描述语言VHDL在现场可编程门阵列(FPGA)上实现具备加密/解密功能的DES核,采用掩码方法对DES硬件结构进行改进,通过仿真和实验进行功能验证,改进的加密算法结构性能符合要求,在理论上具有抗DPA攻击的能力。

**关键词**:现场可编程门阵列;数据加密标准;差分功耗分析;掩码
**中图分类号**:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2011)04-0160-04

# Hardware Design and Implementation of DES Masking Algorithm Based on FPGA Platform

WANG Chuang-wei, DING Guo-liang, YIN Wen-long, CHANG Xiao-long
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

**Abstract**: With the widespread application of FPGA circuit in security field, the DPA-resistant research of FPGA cipher chip is getting much more attention. But most of the present research focus on security of smart card. Aimed at the characteristic of power attack technology and critical technology, especially DPA, to propose improved specify defend approach. By using the VHDL, implement a DES core which has encode/decode function based on FPGA. After applying the masking technique on FPGA, improve the DES hardware structures. It was validated by simulation and experiment. The results show that the design satisfys the demand which has the ability of the DPA resistance in theory.

**Key words**: FPGA; DES; DPA; MASK

## 0 引 言

随着通信技术和网络技术的飞速发展,对于数据传输安全性的要求也随之增强,因此人们提出了很多数据加密算法,相比之下,硬件实现的加密算法则在速度上有着强大的优势。FPGA(Field Programmable Gate Array,现场可编程门阵列)由于其高性能、低价格、快速的开发速度、方便的编程方式等原因得到了广泛的应用。DPA(Differential Power Analysis,差分功耗分析)攻击对FPGA密码芯片造成了极大的威胁[1],已经受到了广泛的关注。文中以FPGA为平台,借助相关工具软件实现DES加密芯片的安全硬件结构设计。

## 1 基于FPGA的DES加密核设计

加密核分为三个模块:数据发送模块、数据接收模块和DES加密模块,三个模块均通过VHDL语言编程,经FPGA设计工具处理后下载到FPGA芯片中进行功能实现。

### 1.1 DES加密模块设计

DES加密模块在工作过程中可由DES_complete主模块来选择调用快速算法模块DES_fast或最小面积算法模块DES_small,加解密模式由信号encrypt_flag控制。在设计中,先将密钥选择及各种变化、置换均模块化,然后将轮运算函数des_round也模块化设计。当选择快速算法模块时,轮运算函数des_round进行16个轮次的完全相同的迭代,即采用一个16级的流水线来实现,每一轮参数配置好后,生成下一轮的结果,每一轮的算法结构都预设好。

### 1.2 接收模块设计

接收模块设计:RST是系统复位信号;分频时钟clk_out由波特率发生器产生;rxd是由来自PC机的串行数据;在rxd_compout信号控制并行数据转换后输出;rxd_out[7:0]是接收模块将接收到的串行数据转

**收稿日期**:2010-08-28;**修回日期**:2010-12-09
**基金项目**:国家高技术研究发展计划(863)(2007AA01Z454)
**作者简介**:王创伟(1980-),男,硕士,从事智能诊断与检测、信息安全等方面研究。

换成的并行数据。该模块具体的工作方式如下:串口处于全双工[2]工作状态,PC 机首先向 FPGA 发送一帧数据协议,数据头 0x11,0x99 后接 8 个字节的数据,FPGA 接收到数据以后将数据原封不动发送给 PC 机,用于调试接收程序。模块实现了一个收发一帧 10 个 bit(即无奇偶校验位)的串口控制器,10 个 bit 是 1 位起始位,8 个数据位,1 个结束位。串口的波特率由程序中定义的 div_par 参数决定,更改该参数可以实现相应的波特率。程序设定的 div_par 的值是 0x104,对应的波特率是 9600。

### 1.3　发送模块设计

发送模块相对于接收模块来说比较容易处理,只要每隔 16 个 CLK16X 周期输出 1 位即可。发送模块具体工作方式如下:当发送数据装载到发送保持寄存器后,串行数据将自动使能从而进行数据传输。当 UART 被复位信号复位以后,rxd[7:0]读取 8 位并行数据,同时检测输出起始位之间的逻辑 1,当检测到输出起始位为 0 时,开始发送数据。首先一个开始位被发送出去,同时发送数据由发送保持寄存器装载到发送移位寄存器中,而将数据以波特率时钟逐位发送出去,并按照线性控制寄存器的要求加上停止位。并行数据发送完毕后,输出停止位逻辑 1,其时钟、帧结构配置和工作过程与接收模块类似。

### 1.4　仿真及实验验证

加密核设计完成后,采用 Xilinx 公司的 ISE Foundation 10.1 软件进行综合实现后功能仿真,根据文献[3]中的算法,采用 16 进制输入,00FF00FF00FF00FF 作为明文,FF00FF00FF00FF00 作为密钥,加密后的密文应为 8234C3738EE42FBD。因此,采用以上的数据作为测试向量,对设计进行了测试。测试结果表明:加密结果一致,将密文作为输入,采用相同的密钥,可以输出一致的密文 00FF00FF00FF00FF,因此本设计的加密/解密功能完全正确。

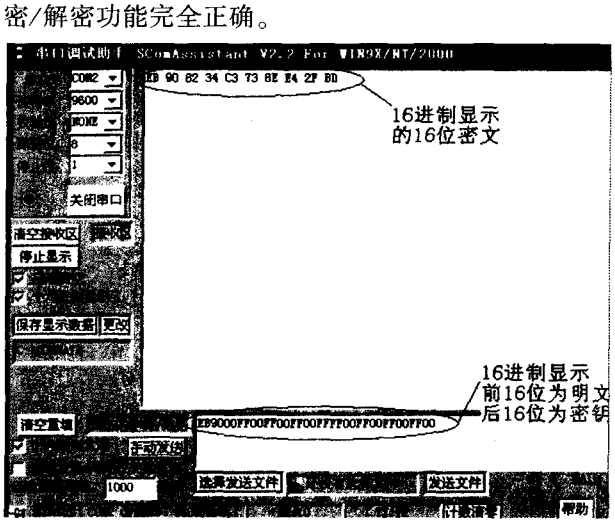


图 1　DES 加密核板上验证结果

仿真完成后,采用 Xilinx 公司的 SPARTAN-3A 开发板,在上一步综合、仿真的基础上进行实现,通过 ISE 软件下载至 xc3s700a FPGA 芯片中,通过串口调试软件输入明文和密钥,经通用异步收发器(Universal Asynchronous Receiver Transmitter,UART)发送到 FPGA 密码芯片中,经过加密后,密文经 UART 通过串口发送到计算机上,实现加密结果的输出,如图 1 所示,在加密模式下,加密核的输出结果和仿真结果一致,进一步验证了加密核的功能正确性。

## 2　DPA 及掩码技术介绍

### 2.1　针对 DES 算法的差分功耗分析

DPA 是最强大的旁路攻击方法之一,而且它使用的资源非常少,易于进行[4]。DPA 攻击不需要实现细节的具体知识,它在分析过程中利用统计学方法找出秘密参量和功率消耗之间精细的统计相关性[5,6]。DES 密码算法及其使用的表格、函数皆为公开数据,惟一的不公开数据仅剩主密钥,因此 DES 算法的安全依赖于主密钥的安全。DES 加密算法是轮迭代的处理过程,正是这种多次循环的迭代,使得芯片在运行该算法的过程中功耗呈现某种特征。对于攻击者来说只要破解一轮的密钥就可以倒推出主密钥中的 48 位,剩下的 8 位可用穷举法获得。DPA 技术是先破解 DES 的子密钥权进而破解 DES 主密钥。攻击者可以监测并统计芯片的功耗曲线并通过最大似然估计分析找出密钥[7],因此即使是硬件实现的 DES 加密芯片对 DPA 攻击都显得很脆弱,文献[8]指出,和普通智能卡相比,FPGA 芯片上实现的 DES 加密算法具备一定的防护能力,但还是被成功攻击。

### 2.2　MASK(掩码)技术的引入

掩码技术[9]主要是通过修改密码算法,使得算法的硬件实现不泄漏密钥信息。即在数据运算之前,将数据 $i$ 与随机数 $r$ 进行位异或操作,得到随机化的数据 $m(m=i\oplus r)$,然后对 $m$ 进行正常的密码运算,最后从获得的运算结果中恢复出正常情况下的密码运算结果。由于随机数是未知的,非法用户无法获得被掩盖的关键信息,可以防止分析关键数据。

DES 算法掩码方法包括逻辑掩盖和加法掩盖方法。一种为逻辑掩盖,用数据位的异或操作运算;一种为算术掩盖,用 $2^{32}$ 模的加法运算。文中采用逻辑屏蔽的方法,以随机数 $R$ 和要屏蔽的字 $M$ 为例来介绍,操作后的结果是 $M1$,其中 $R$ 是由随机数硬件发生装置产生的随机数,$T$ 是未经掩盖的值,$T1$ 是掩盖后的值。异或掩盖方法仅仅包含逻辑运算单元,其算法过程是:

输入:$(T,R)$,$T1=T\oplus R$

输出:$(D,R)$,$T=D\oplus R$　假定 $R$ 为随机数 1 或

0

(1) $B = L \oplus R$

(2) $D = L \oplus T$

(3) $D = D \oplus B$

易得 : $T \oplus R = \overline{T} \oplus \overline{R}$

## 3 抗功耗攻击 DES 掩码算法 IP 核设计

### 3.1 DES 掩码算法结构设计

文中研究发现,文献[10]提出的屏蔽方法在数据进入 S 盒之前就消除随机数,不能防御后来提出的高阶 DPA 攻击,极易受到二阶 DPA 攻击。为了完全屏蔽密钥,文中对这种掩码方法进行改进来防御 DPA 攻击,基本思想是使得每一轮的输出与输入是用同一个随机数进行的屏蔽,用一个随机数对所有数据进行异或。在数据进入 S 盒之前不恢复密钥,继续保持屏蔽状态进入 S 盒,由于 S 盒是非线性的,为了保证 S 盒的输出将来有机会消除随机数还原得到正确的数据,需要修改原始 S 盒。

DES_Mask 算法是采用 Mask 技术对 DES 运算中的明文和密钥相关中间变量进行掩盖,使与输入明文和存储密钥的相关功耗信息不泄漏出来。具体的 DES 掩码算法过程如下:对一个 64 bit 的明文 M 加密,首先由内部的随机数发生器产生一个 64bit 的随机数 X,将 M 和 X 通过异或运算生成 M ⊕ X 作为加密的初始值进行运算。

和普通 DES 相比较,除 F 函数和 S 盒有变化外,算法结构有以下变化:

(1)1 到 15 轮加(解)密计算时,右 32 位作为下一轮左 32 位时,要先与随机数 MASK 的变形值 MASK2 进行异或运算。

(2)第 16 轮运算时,左右 32 位互换后都要和 MASK2 进行异或运算。

(3)第 16 轮运算完后,输出密文前要和随机数 MASK 进行异或运算。

### 3.2 改进 F 函数模块

标准的 DES 算法采用 8 个不同的 S 盒,因此修改的 DES 算法也要对应 8 个修改的 S 盒,改进掩码算法和普通掩码算法的主要区别是:改进掩码算法的开始和结束时对消息进行屏蔽,S 盒也发生变化,S 盒替换是非线性的,为了适应 Mask 算法需要修正。在 DES 掩码算法中采用了修正过的 S 盒:$SBox_2(A) = SBox(A \oplus E(MASK1_R)) \oplus P^{-1}(MASK1_L \oplus MASK1_R)$

这里 $P^{-1}$ 表示置换 P 的逆运算,E 为明文扩展置换。在实际运算中,可以看到 MASK 经 IP 变换后,左 32 位为 $MASK1_L$,右 32 位为 $MASK1_R$,MASK2 为 $MASK1_L$ 和 $MASK1_R$ 的异或结果。图 2 是采用掩码方法时的 F 函数。

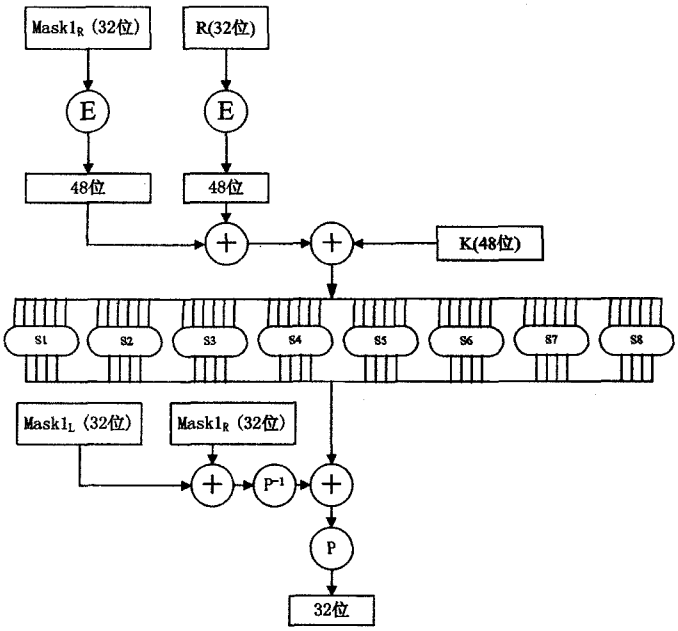


图 2 DES 掩码算法 F 函数结构

### 3.3 伪随机数生成模块

基于 FPGA 的伪随机数发生器[11]基本原理是利用奇数个反相器组成振荡器作为随机数发生器的噪声源,因为 FPGA 自身存在信号传输抖动的缺点,所以多个反相器组成振荡器输出也不是很稳定的时钟信号,每个振荡器输出不是相同的,可以得到理想的随机数列,图 3 是其原理图。

振荡器输出通过 D 触发器进行采样输出,采样频率是 fs,然后多个采样输出结果经过异或门之后再通过一个 D 触发器进行采样,采样频率还是 fs,以上就是简单随机数发生器原理。

根据原理图进行如下设计:文中采用的抽样频率 fs 为 50MHz,用 3 个反相器组成一个振荡器,共用了 25 个振荡器,为了避免 ISE 综合器将振荡器进行一定的优化从而背离当初的设计,所以在代码中添加了属性语句,用于保证网络不被优化掉,通过 ISE 工具完成设计输入和实现。

### 3.4 DES 掩码算法功能仿真结果

使用 ISE 集成的 HDL Editor 完成 DES 掩码算法 RTL 代码的编写,同时设计 Testbench(测试激励文件)验证电路的正确性,使用 Xilinx FPGA 开发工具 ISE10.1 及其组件完成综合实现后进行仿真,DES_Mask 算法的仿真结果和不加掩码的 DES 算法结果一致,但 16 轮运算后输出的中间结果发生了变化。在实际仿真软件中,因掩码的影响,两种算法每一轮的运算结果均不一样,达到了掩码的效果,因此通过仿真可以

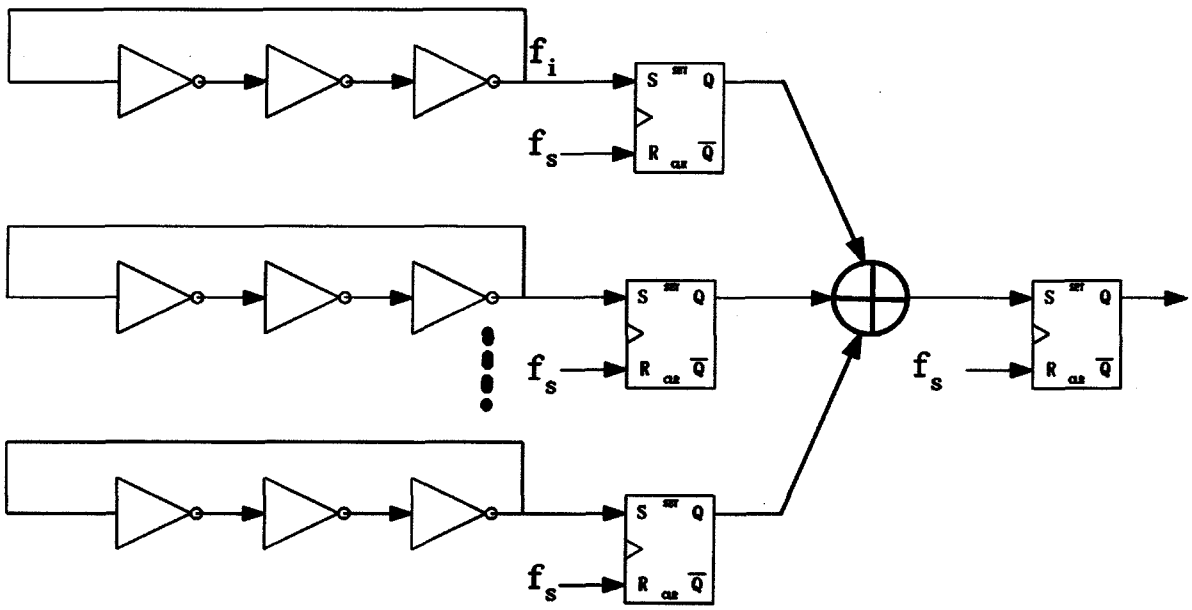


图 3　随机数生成器原理图

反映掩码算法功能正确,而且除输入和输出外,和 DES 相比,与密钥相关的所有中间结果均发生了变化,从 DPA 攻击方法进行理论分析可知,攻击后只能得到错误的猜测密钥。

由综合得出的报告发现,DES 加密算法的 slice 及 LUT 等硬件资源占用率为 10%,而 DES 掩码算法的硬件资源占用率为 12%,掩码算法的面积没有太大变化。仿真后将两种加密核下载至 SPARTAN-3A 开发板中运行发现,系统均能稳定地工作在 40MHz,加解密速度达到 2.56Gbps。总之,和文献[12]设计相比,掩码加密系统在性能上没有降低,只是面积上略有增加。

## 4　结束语

DES 算法是密码体制中的一个重要算法,DES 加密模块是许多安全系统的核心模块,因此在 FPGA 芯片上设计一个实用化的防止 DPA 攻击的 DES 核具有重要的意义。以速度和资源作为着眼点,通过对 DES 的实现方法做适当的改进,将其中间变量进行掩码,从而避免被预测。而且即使局部变量可能被预测到,但是因为 FPGA 芯片本身和掩码电路中增加了很多随机性的功耗,降低了密钥与中间状态的相关度,所以其抗 DPA 攻击的能力大大加强,增加了系统应用的安全性。

**参考文献:**

[1] 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.

[2] 张　明. 基于 FPGA 的 UART 控制器的多模块设计与实现[J]. 中国科技信息,2006(16):138-140.

[3] 陈鲁生,沈世锰. 现代密码学[M]. 北京:科学出版社,2002.

[4] Kocher P, Jaffe J, Jun B. Differential power analysis[C]// Proc. of Advances in Cryptology - CRYPTO '99 . [s. l. ]: Springer-Verlag,1999:388-397.

[5] 石　伟,戴　葵,童元满,等. 防 DPA 攻击的标准单元库的设计与实现[J]. 微电子学与计算机, 2007,24(2):51-54.

[6] 张　涛, 范明钰, 郑秀林. 一种抗旁路攻击的自愈密码系统设计[J]. 计算机应用研究, 2008,25(9): 2829-2830.

[7] 张　涛, 范明钰. 一种面向密码芯片的旁路攻击防御新方法研究[J]. 软件学报, 2008,19(11):2990-2998.

[8] Tiri K, Verbauwhede L. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation[EB/OL]. 2004-02. http://www. cosic. esat. kuleuven. be/publications/article-697. pdf.

[9] Messerges T S. Securing the AES finalists against power analysis attacks[C]//International Workshop on Fast Software Encryption. New York, NY, USA:[s. n. ],2000:150-164.

[10] 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.

[11] 李　超,王红胜,陈军广,等. 加强计算机终端信息安全的两种解决方案[J]. 计算机技术与发展,2009,19(1):165-167.

[12] 王简瑜,张鲁国. 基于 FPGA 实现 DES 算法的性能分析[J]. 微计算机信息,2007,23(8):217-218.