基于 FPGA 平台的抗 DPA 攻击电路级防护技术研究

王创伟，原　亮，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：随着现场可编程门阵列(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。在研究各种电路级安全防护技术的基础上，采用硬件宏的方法将双轨和预充电技术应用于 FPGA 芯片的数据加密标准算法(DES)硬件结构，通过 DPA 攻击实验后发现，未加防护措施的 DES 加密系统难以抵御 DPA 攻击，而加防护措施的加密系统具有抗 DPA 攻击的能力。

关键词：FPGA；差分功耗分析；数据加密标准；双轨；预充电
中图分类号：TP309.7　　**文献标识码**：A　　**文章编号**：1004-373X(2010)09-0001-03

Pretection Technique of Anti DPA-attack Circuit Based on FPGA Platform

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

Abstract: With the widespeard application of field programmable gate array(FPGA) chip in the securtity field, the anti DPA-attack research of FPGA ciphering chip are getting much more attention, but most of the present research achievements focus on the security of smart cards. Based on the protection technique research of circuit, the dual-rail and pre-charge technique is applied in the data encryption standard(DES) hardware structure of the FPGA chip with the hard macros method. The attacking experiment of DPA demonstrates that without pretecting measure DES enciphering system can't defend DPA, but enciphering system using pretecting measure has the ability to resist DPA-attack.

Keywords: FPGA; differential power analysis; DES; dual-rail; precharge

0　引　言

近年来，现场可编程门阵列(Field Programmable Gate Array，FPGA)由于其高性能、低价格、高开发速度、方便的编程方式等特点得到了广泛的应用。但对 FPGA 进行 DPA(Differential Power Analysis，差分功耗分析)[1]攻击已经成为 FPGA 应用中信息安全的主要威胁之一，受到了广泛的关注。

DPA 是 SCA(Side Channel Attacks，旁路攻击)[2]技术的一种，其攻击思想为：以电路的功耗特性为基础，利用功耗与内部密钥的关系，将大量采样到的包含该内部密钥运算的功耗波形数据根据所猜测的密钥进行划分，使得所划分的两部分具有不同的功耗特性。最后，对两部分的功耗数据相减得到功耗差分曲线，如果猜测正确，差分曲线将出现明显的尖峰[2]。

因此，进行 DPA 攻击的根本原因是电路逻辑表示的不对称性引起的。本文将应用 FPGA 的自身结构特点，结合目前常用的抗 DPA 攻击的电路级防护技术，深入研究与分析在 FPGA 平台上实现针对 DPA 攻击的电路级防护技术。

收稿日期：2009-12-15
基金项目：国家 863 项目“密码芯片电磁信息泄漏侧信道攻击与防护技术研究”(2007AA01Z454)；国家自然科学基金项目“集成电路芯片电磁泄漏旁路攻击机理及解密研究”(60571037)

1　FPGA 上的电路防护技术

1.1　FPGA 的底层结构

FPGA 的简化结构如图 1 所示。FPGA 内部最主要的、设计工程中最需关注的部件是 CLB(Configurable Logic Block，可配置逻辑块)，IOB(Input/Output Block，输入/输出块)，Block RAM(块 RAM)、DCM(Digital Clock Manager，数字时钟管理器)和 Multiplier(乘法器)。其中 CLB 是 FPGA 具有可编程能力的主要承担者，Virtex-5 的一个 slice 的主要组成单元包括 4 个6 输入查找表、4 个触发器和若干个选择器。

1.2　双轨电路技术的实现

双轨电路技术是指无论是输入还是输出都是用两根线来表示的。由图 2 可见，在 SDDL 与门[3]中，信号 A就由 A 和 $\overline{A}$ 共同表示，而输出 Z 也由 Z 和 $\overline{Z}$ 表示。在这种表示下，一个变量可以有 4 种不同的逻辑值(0,0)，(0,1)，(1,0)以及(1,1)。SDDL 将(0,1)和(1,0)分别用来表示逻辑 0 和逻辑 1。这样电路内部的逻辑 0 和逻辑 1 就变成了对称的，从而使得各自的功耗

相同。另外,逻辑门还引入了一个 prch 预充电信号。在 prch 有效的情况下,输出是(0,0),这个值也就是变量为预充电时在电路中的表示方式。电路的工作分为两个状态:运算状态和预充电状态。这两个状态交替更换,也就是在 prch 上加载一个固定周期的脉冲。如此一来,电路中变量值的变化就是(0,0)到(0,1)或(1,0),或者是(0,1)或(1,0)到(0,0),每次翻转都是只有一根信号线进行翻转。逻辑 0 和逻辑 1 达到了完全的平衡。

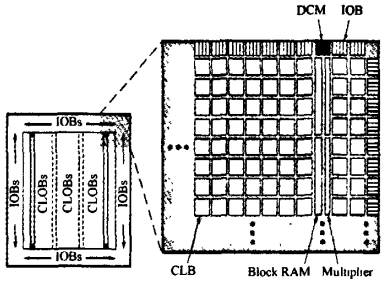

图 1 FPGA 结构图

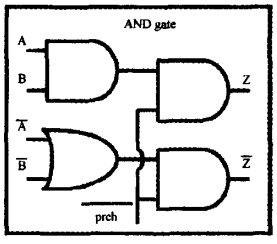

图 2 SDDL 与门

1.3 预充电技术的实现

普通逻辑门不能提供持续转换活动,逻辑门的输入不变将导致门的数据独立。解决这个问题要通过增加预充电电路来提供变换。当时钟为高时,连接预充电电路输入一个预充电相位,连接点变化到逻辑 0;当时钟为低时,电路输入计算相位,实际计算完成。在 FPGA 上采用预充电逻辑的目的是要求在预充电相位期间 slice 的输出必须是逻辑 0,有两种方式来完成[4]。在一个Xilinx 的 slice 中,每个 LUT 后跟着专门的多路选择器和内存单元,可配置为寄存器或锁存器。这里考虑使用多路复用器和内存单元来实现预充电,每种方法各有优点和缺点:

(1) 使用时钟控制的多路复用器来实现预充电功能。将每个片子中单独的内存单元作为寄存器,但是除了寄存器的普通时钟还要分配一个反向时钟。这种方法的缺点是复制一个时钟信号并生成直接和互补信号将明显增加功耗和电路面积,布线也将复杂化。

(2) 使用内存单元作为带有反向使能输入的异步清零锁存器来实现预充电功能。只需要一个单独信号给寄存器和预充电锁存器,预充电功能由连接反向使能输入和锁存器的清零输入实现,使用这种方法的缺点是专门设计的寄存器存储器需要一个单独的 slice。

2 DES 加密模块的实现

要在 FPGA 上实现安全防护结构来确保关键部件的功耗恒定。这里选择从双轨和预充电技术在 FPGA 上实现旁路安全防护逻辑。当前的技术水平需要在 FPGA 上进行精确控制布局和布线[5]。下面从 S 盒硬件宏的实现和 DES 加密核的实现来介绍基于 FPGA 的 DES 加密模块实现。

2.1 S 盒硬件宏的实现

S 盒的设计是 DES 算法关键部分,S 盒设计的优劣将影响整个算法性能。在采用 FPGA 实现时,应从资源和速度的角度出发,有效利用 FPGA 可配置属性,充分考虑器件内部结构,尽可能使两者都达到最优。在设计中,由于综合工具的介入,所输出的网表很难被设计者所理解,同时要找到一种更好的方法来控制组合电路,因此要建立硬件宏模块[6],简称硬宏。这与传统的设计流程不同之处是要充分利用 FPGA Editor 的功能,目的是从 FPGA 底层结构的配置上实现双轨和预充电技术。

通过 Xilinx 提供的 FPGA Editor 工具,首先读入布局布线后输出的 NCD 文件,并将其转化为新的 NVD 文件,再送往 BitGen 软件,进行布局布线的优化,最终在 FPGA 内部来建立目标电路,把它存为一个宏文件便于在上层进行调用。要注意两个问题:建立硬宏需要进入到 slice 内部,准确控制 Slice 内部的器件选择和器件之间的连线,防止设计出错;宏的功能验证要建立仿真模型,直接编写一个行为仿真模型后在上层设计中调用这个仿真模型,要确保仿真模型和宏之间的一致性。

2.2 DES 加密核的实现

DES 算法的基本流程如下:首先,输入明文通过初始置换,将其分成左、右各为 32 位的两个部分,然后进行 16 轮完全相同的运算。经过 16 轮运算后,左、右半部分合并在一起经过一个末置换(初始置换的逆置换),于是整个算法结束。在每一轮运算中,密钥位移位,然后再从密钥的 56 位中选取48 位。通过一个扩展置换,将数据的右半部分扩展为 48 位,并通过一个异或操作与一个48 位密钥结合,通过 8 个 S 盒将这 48 位替代成新的 32 位数据,再通过一级置换操作,这四步操作即为函数 f。

S 盒是 DES 中的非线性模块,直接决定 DES 算法的安全性。在函数 f 的实现中,采用上面的思路,使用例化调用了 S 盒。DES 加密核的 VHDL 设计思路如下:首先调用库函数构造 ROM,然后使用 VHDL 语句进行行为描述。这种方法要结合器件的内部结构,对于

小容量的 ROM 采用数组描述，大容量的 ROM 应采用元件的方式来实现[7]。在 VHDL 设计中，库函数、子程序的调用以及元件的调用和使用间接变量，都是影响速度的主要因素。由此得到 DES Core 的接口定义如下：

```
ENTITY des56 IS
PORT(
indata    :IN     std_logic_vector(0 TO 63);
inkey     :IN     std_logic_vector(0 TO 63);
outdata   :OUT    std_logic_vector(0 TO 63);
decipher  :IN     std_logic
ds        :IN     std_logic
clk       :IN     std_logic
rst       :IN     std_logic
rdy_next_next_cycle  :OUT     std_logic
rdy_next _cycle      :OUT     std_logic
rdy                  :OUT     std_logic
);
END des56;
```

3　攻击实验的对比与分析

3.1　FPGA 加密芯片攻击试验平台建立

目前 FPGA 的种类很多，但其中有大于 50%的份额被 Xilinx 公司抢占，在此选用 Xilinx 公司的 Virtex-5 (ML501)，对其他种类的 FPGA 的攻击和此类似。ML501 在工作时需要 3 个工作电压：内核电压(1.2 V)、辅助电压(2.5 V)、I/O 电压(3.3 V)，而 ML501 芯片的所有地线是并结在一起的。对 FPGA 攻击的实验的原理图如图 3 所示，示波器(Tektronix DPO4104，1 GHz BW，5 Gsample/s)的 2 通道接收 Virtex-5(ML501)加密模块的触发信号，在内核电压和芯片之间置一个电流探针(Tektronix CT-2，1.2 kHz～200 MHz)，1 通道用电流探针测试内核的功耗变化。攻击过程如下：在 PC 机上生成 64 位随机明文，通过串口发送至 FPGA。FPGA 收到明文后利用存储在其中的密钥对明文进行 DES 加密，并在第 16 轮加密操作时对示波器产生数据采集的触发信号。在进行数据采集时其实质是要采集内核电流所引起的功耗变化，并将数据通过 USB 总线送至 PC 机，最后在 PC 机上运行分析程序攻击出 64 位的密钥。

3.2　对 FPGA 加密芯片的攻击

设定明文输入和电流数据采样为 500 组，采样深度 100 000 点，采样频率为 500 MSPS。在相同的试验环境下，对带有防护结构和不带防护结构的两种 DES 的加密结构进行功耗测量，同时根据密钥的推测将明文分类，计算各类的平均功耗，然后相减，可以得到差分功耗分析曲线。

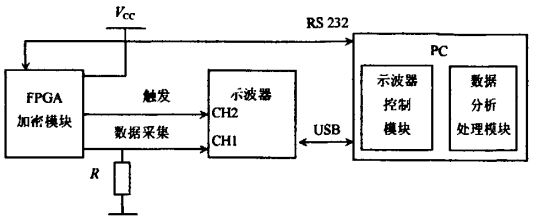

图 3　DPA 实验电路原理图

试验后发现对不带防护结构的 ML501 FPGA 芯片进行攻击时，当子密钥块猜测正确时，功率差分曲线出现明显的尖峰，采用相同的方法可以攻击出其他子密钥块，由此可以获取第 16 轮的子密钥 K16(48 位)，攻击成功。对带防护结构的芯片攻击时，功率差分曲线基本是平缓的，波动非常小，也没有明显的尖峰存在，可见 DPA 攻击对带有防护结构的 FPGA 无效。

4　结　语

由以上 DPA 攻击试验表明了 FPGA 实现 DES 加密算法对 DPA 的脆弱性，而采用双轨和预充电防护技术的 FPGA 加密芯片具有较好的抗 DPA 攻击能力。这也说明利用 FPGA 底层开发工具通过硬件宏方法能在 FPGA 硬件上实现安全防护技术的拓展，对开展芯片的安全防护工作的研究具有重要意义。

参　考　文　献

[1] KOCHER P, JAFFE J, JUN B. Introduction to differential power analysis and related attacks[J]. IEEE Trans. on Electron Devices, 1998, 50(2): 462-470.

[2] 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)：172-172，176.

[3] CLAVIER C, CORON J, DABBOUS N. Differential power analysis in the presence of hardware countermeasures[J]. CHES 2000, Lect. Notes Comput. Sci., 1965, 21(13): 252-263.

[4] TIRI K, VERBAUWHEDE I. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation[C]// Proc. of Design Automation and Test in Europe Conference. [S. l.]: DATE. 2004: 246-251.

[5] 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.

[6] 李永彬，雷菁. DES 加密算法的高速 FPGA 实现[J]. 电子工程师，2005，31(7)：39-41.

[7] 王峰，周学海，陈艾，等. 基于部分重构技术的加密算法实现研究[J]. 电子学报，2007，35(5)：959-964.

作者简介：王创伟　男，1980 年出生，在读硕士。主要研究方向为智能诊断与检测。
原　亮　男，1955 年出生，教授。主要研究方向为智能诊断与检测。

基于FPGA平台的抗DPA攻击电路级防护技术研究

作者： 王创伟， 原亮， 丁国良， 尹文龙， 常小龙， WANG Chuang-wei， YUAN Liang， DING Guo-liang， YIN Wen-long， CHANG Xiao-long

作者单位： 军械工程学院,计算机工程系,河北,石家庄,050003

刊名： 现代电子技术 ISTIC

英文刊名： MODERN ELECTRONICS TECHNIQUE

年，卷(期)： 2010，33(9)

被引用次数： 0次

参考文献(7条)

1. KOCHER P. JAFFE J. JUN B Introduction to different ialpower analysis and related attacks 1998(2)

2. 曹建国. 王丹. 王威 基于RSA公钥密码安全性的研究 2007(1)

3. CLAVIER C. CORON J. DABBOUS N Differential power analysis in the presence of hardware countermeasures 1965(13)

4. TIRI K. VERBAUWHEDE I A Logic Level Design Me-thodology for a Secure DPA Resistant ASIC or FPGA Implementation 2004

5. 王简瑜. 张鲁国 基于FPGA实现DES算法的性能分析 2007(8)

6. 李永彬. 雷菁 DES加密算法的高速FPGA实现 2005(7)

7. 王峰. 周学海. 陈艾 基于部分重构技术的加密算法实现研究 2007(5)

相似文献(3条)

1. 期刊论文 丁国良. 赵强. 褚杰. 邓高明. DING Guo-lang. ZHAO Qiang. ZHU Jie. DENG Gao-ming FPGA密码芯片差分功耗分析仿真研究 -计算机工程与应用2007,43(22)

在分析FPGA组成结构特点的基础上,根据FPGA功耗产生的机理,提出了一种FPGA功耗模型.针对DES加密的DPA,实现了DPA仿真平台,并利用该模型和仿真平台验证了FPGA实现DES加密算法对DPA攻击的脆弱性.

2. 期刊论文 邹程. 张鹏. 邓高明. 赵强 AES密码电路抗差分功耗分析设计 -计算机工程与应用2009,45(36)

针对差分功耗分析(DPA)攻击的原理及特点,分析了高级加密标准(AES)的DPA攻击弱点,采用掩盖(Masking)的方法分别对AES算法中字节代换部分(SubBytes)及密钥扩展部分进行了掩盖,在此基础上完成了AES抵御DPA攻击的FPGA硬件电路设计.通过对该AES的FPGA电路的差分功耗攻击实验验证,该方法能够很好地抵抗DPA攻击.

3. 学位论文 晏楠 公钥密码的边界信道攻击研究 2006

上世纪90年代中期以来，利用密码算法芯片的物理特性实施边界信道攻击引起了国内外密码学界的极大关注，已经成为密码分析学发展最为迅速的领域之一。实际应用的密码算法通常用专用硬件、软件或固件来实现，如ASIC、FPGA、DSP或智能卡等密码算法芯片（以下简称密码芯片），这种芯片在运行时有可能泄漏某些与密钥相关的部分信息，称为边界信道信息。典型的边界信道信息包括密码芯片的执行时间、能量消耗、电磁辐射、出错信息等。以前，人们对密码算法的分析主要集中在对其数学变换的分析上。但在近年来，随着集成电路和智能卡技术的发展以及嵌入式系统的大规模应用，边界信道攻击由于其成功的攻击效果和广泛的用途，正受到人们越来越多的关注。边界信道攻击的主要形式有：时间攻击（Timing Attack）、功耗分析（Power Analysis）和故障分析（Fault Analysis）。

本文立足于密码芯片安全性的实际需求，从算法研究和软件设计等方面展开工作，在攻击方法和防御方法两个方面对公钥密码算法的时间攻击、功耗分析和故障分析进行了研究。针对当前广泛应用的RSA和ECC体制以及其中的核心运算单元，分析了时间攻击、简单功耗分析、差分功耗分析和故障的各种攻击方案，并有针对性的分析了各种防御攻击的密码算法实现方案，从而为设计能够有效抵御主要边界信道攻击的密码芯片及相应软件，提供理论依据和实现指南。

本文以RSA体制为研究重点，提出了RSA体制防御时间攻击和多信道攻击的新方案：第一，在对时间攻击和原有抗击方法进行分析的基础上，提出两种新的防御方法，将RSA算法由确定算法改造为随机算法，这样不但保证了算法安全性，而且可以大大提高算法的执行效率。第二，针对RSA-CRT体制面临的多信道攻击，提出了有效抗多信道攻击的实现方案。该方案通过综合使用去除条件语句、盲化消息和盲化指数等三种防御思想，能够同时防御利用简单功耗分析、时间攻击、故障分析和差分功耗分析的多信道攻击。