FPGA 密码芯片差分功耗分析仿真研究

丁国良,赵 强,褚 杰,邓高明
DING Guo-liang,ZHAO Qiang,ZHU Jie,DENG Gao-ming

军械工程学院 计算机工程系,石家庄 050003
Dept. of Computer Engineering,Ordnance Engineering College,Shijiazhuang 050003,China
E-mail:DGL998@163.com

DING Guo-liang,ZHAO Qiang,ZHU Jie,et al.Research of simulation DPA for FPGA cryptographic chips.Computer Engineering and Applications,2007,43(22):103-105.

Abstract: Through analyzing architectural features of FPGA,a power consumption model of FPGA on the basis of the mechanism for power consumption is put forward.A DPA simulation platform is realized for DPA to DES.The model and platform validate the vulnerability of the realization of DES with FPGA for DPA attacks.

Key words: side-channel attacks;power leakage model;Differential Power Analysis(DPA);FPGA

摘 要: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。

关键词:旁路攻击;功耗泄漏模型;差分功耗分析;FPGA
文章编号:1002-8331(2007)22-0103-03 **文献标识码**:A **中图分类号**:TN309.7

1 引言

差分功耗分析(Differential Power Analysis,DPA)是一种快速、低成本、可实施的密码芯片攻击技术,可以有效获取密码芯片中的关键数据和密钥,已对密码芯片的安全性提出了严重的挑战。自 1998 年 Paul Kocher 等人提出后[1],DPA 得到了国内外学者和厂商的广泛关注。目前国际上的研究成果大都集中在针对智能卡的攻击与防护上,但随着 FPGA 芯片在安全领域上的广泛应用,有关 FPGA 密码芯片的 DPA 也越来越关注[2]。因此针对 FPGA 密码芯片开展功耗分析与抗功耗分析的研究具有重要意义。本文在描述 FPGA 芯片工作时产生功耗泄漏的机理和 DPA 实现的基础上,针对 FPGA 加密芯片实现 DES 加密算法建立了寄存器级的功耗模型和仿真平台,进行了 DPA 仿真攻击实验,并给出了 DPA 仿真结果。

2 FPGA 芯片功耗分析

目前 FPGA 主要分为 SRAM 型、EEPROM 型和 Anti-fuse 型 3 种,其中 SRAM 型应用最为广泛,例如有 Xilinx 公司的 Spartan、Virtex 系列、altera 的 ACEX、APEX 等系列。从芯片的组成结构来看,SRAM 型一般采用查找表(LUT)结构。以 Xilinx 公司的 Spartan II 系列为例,该类芯片主要由 CLB、I/O 块、RAM 块和可编程连线等组成。一个 CLB 包括 2 个 slices,每个 slice 包括两个 LUT、两个触发器和相关逻辑。Spartan II 使用 4 输入的 LUT,每一个 LUT 可以看成一个有 4 位地址线的 16×1 的 RAM。当使用原理图或 HDL 语言描述一个逻辑电路以后,FPGA 开发软件自动计算逻辑电路的所有可能的结果,并可将这些信息保存在专用配置芯片中。加电后,FPGA 首先从配置芯片下载配置信息至 LUT,完成配置后,输入信号进行逻辑运算就等于输入地址进行查表操作,找出 LUT 相应单元中的内容,然后输出相应结果。

从半导体工艺技术上看,几乎所有的 SRAM 型 FPGA 器件都是采用 CMOS 技术。因此,该型 FPGA 的功耗主要分为静态和动态功耗两个部分。静态功耗是由于穿越 FPGA 中晶体管氧化栅的漏电流带来的功耗,动态功耗是由于 FPGA 的容性负载进行充电和放电所需的功耗。动态功耗占总功耗的大部分。以最简单的 CMOS 逻辑门电路倒相器(见图 1)为例分析门电路的功耗[4]:第一部分为倒相器发生 0 到 1 或 1 到 0 变化时从源到地的短路电流功耗 P_{sc},这部分大约占整体功耗的 15%;第二部分是对电容 C_L 充、放电时的动态功耗 P_{sw},$P_{sw}=C_L V_{cc}^2 P_{(0\to1)} f$,式中 C_L 为负载电容,V_{CC} 为电源电压,$P_{(0\to1)}$ 为门电路发生从 0 到 1 翻转的概率,f 为输入更新的频率,这部分功耗是 CMOS 功

IN	OUT
0→0	0
0→1	discharge
1→0	charge
1→1	0

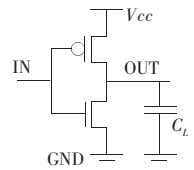

图 1 CMOS 倒相器和充放电逻辑

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60571037)。

作者简介:丁国良,男,博士生,副教授,主要研究方向为智能检测与故障诊断、集成电路安全与防护、演化硬件;赵强,男,博士生导师,教授,主要研究方向为信息安全、集成电路安全与防护;褚杰,男,博士生,主要研究方向集成电路安全与防护、芯片级自修复研究。

耗的主要部分,大约占整体功耗的 80%;此外还有 MOS 管中的反向泄露电流产生的静态功耗 P_{lk},这部分功耗最小,约占整体功耗的 5%。因此,CMOS 电路的功耗模型可表示为 $P_t=P_{sw}+P_{sc}+P_{lk}$。由此可以看出,CMOS 集成电路芯片的功耗与芯片内部逻辑门的数量和翻转的频率密切相关。在 FPGA 中,其功耗与使用资源的数量和时钟频率成正比。

除 P_t 之外,芯片和电路中还存在各种噪声,外部噪声、本征噪声、量子噪声和算法噪声,这些噪声可以认为是正态分布的随机变量。因此,在某一时刻 t,芯片的总功耗是该时刻 k 个门电路的功耗及各种噪声功耗 $N(t)$之和:

$$P(t)=\sum_{i=1}^{k}P_t(i,t)+N(t) \tag{1}$$

大量的 DPA 实验证明了集成电路功耗与数据操作是密切相关的[1,2]。但是,FPGA 芯片的功耗和数据的相关性,与智能卡和单片机不完全相同,不仅与功耗的种类有关,而且还与 FPGA 的组织结构有关。以 Xilinx Virtex II 为例,芯片中的 CLB、RAM 等核心电路使用 2.5 V 电压,而 I/O 块使用 3.3 V 电压;文献[5]研究表明,在该类芯片的总动态功耗中,内连接线路占 60%,时钟占 14%,逻辑电路占 16%,I/O 块占 10%。而与数据相关的顺序从高到低的依次为逻辑电路、内连接线路、I/O 块和时钟。其中逻辑电路、内连接线路所占比例最大,且与操作数据的关系最为紧密。因此在实际进行功耗建模时可以只考虑逻辑电路、内连接线路的动态功耗。同时,由于静态功耗、短路功耗与噪声在整体功耗中所占比例较小,此时可将式(1)简化为:

$$P(t)=\sum_{i=1}^{n}P_t(i,t) \tag{2}$$

3 差分功耗分析

DPA 是一种有效的密码攻击技术。其理论基础是:在加密过程中芯片要消耗能量,而消耗的能量随处理的数据不同会有微小的变化,根据这种变化可以确定所处理的数据是 0 还是 1,从而有可能猜出加密算法中所使用的密钥。

在分析过程中首先建立一个假想模型 D,D 代表加密操作过程的某一位的值 0 或 1。该函数定义规则如下:如果密码运算中存在一个函数等式

$$F(temp,K_b)=CT \tag{3}$$

其中 CT 为密文,K_b 为 b 位子密钥,$F()$是一个确定函数,那么由式(3)可以得到另一个函数等式:

$$D(CT,K_b)=temp \tag{4}$$

如果 $temp$ 只有 1 bit 时,可将 $D(CT,K_b)\rightarrow\{0,1\}$称为一个判别函数。它的意义在于,$K_b$ 的正确与否,同根据式(3)计算得到的 $temp$ 正确与否密切相关,也就与计算 $temp$ 产生的功耗密切相关。因此,DPA 攻击方法如下:

步骤 1 首先进行 N 次密码运算,获取:

(1)N 个随机的明文输入 $PT_i(1\leqslant i\leqslant N)$;

(2)$S_i[j]$:对第 i 次加密运算产生的功耗进行离散采样形成的功耗数组,其中 $1\leqslant i\leqslant N$,j 表示采样的时间点;

(3)对应于 PT_i 的相应密文输出 $CT_i(1\leqslant i\leqslant N)$;

步骤 2 定义一个与密钥密切相关的函数 $D(CT_i,K_b)$,并令 $K_b=0$,将基于采样时间点 j 的信号数组集合$\{S_i[j]|1\leqslant i\leqslant N\}$分成两个子集合:

$$S_0=\{S_i[j]|D(\cdot)=0,1\leqslant i\leqslant N\},S_1=\{S_i[j]|D(\cdot)=1,1\leqslant i\leqslant N\} \tag{5}$$

步骤 3 计算集合 S_0 与 S_1 平均功耗值($|S_0|+|S_1|=N$):

$$A_0[j]=\frac{1}{|S_0|}\sum_{S_i[j]\in S_0}S_i[j]\quad A_1[j]=\frac{1}{|S_1|}\sum_{S_i[j]\in S_1}S_i[j] \tag{6}$$

并得到 DPA 差分信号数组

$$T[j]=A_0[j]-A_1[j] \tag{7}$$

步骤 4 如果 $T[j]$代表的差分功耗曲线上在某个位置出现明显的尖峰。那么表示 K_b 猜测正确,继续执行步骤 5。否则,修改猜测,令 $K_b=K_b+1(K_b\leqslant 2^b)$,转步骤 2,循环运行直到 K_b 猜测正确。

步骤 5 按上述方法获取所有的子密钥块以后,计算得到整个密钥。

4 DPA 的仿真实现

4.1 功耗模型

(1)汉明距离模型

如果在加密算法运行过程中某一数据 x 经运算直接转换为 x',那么该运算产生的功耗可以用 x 和 x'之间的汉明距离表示,即 $P_{DH}=kH(x\oplus x')$。其中,P_{DH} 表示运算产生的功耗值,H 代表汉明重量,$H(x\oplus x')$即为 x 和 x'之间的汉明距离,k 是一个常量因子。

(2)汉明重量模型

在某些情况下,汉明距离模型可以由于对系统实现细节的了解而被加以简化。例如,对于预置数据为全 0 的寄存器,功耗依赖于输入线上数据 x 的汉明重量,即 $P_{WH}=kH(x)$。其中,P_{WH} 表示功耗,$H(x)$为总线数据 x 的汉明重量,k 是一个常量因子。

4.2 寄存器级功耗仿真

由前面分析可知,某一时刻 FPGA 芯片的功耗在门电路一级的计算值,可以用正在进行充放电的 CMOS 门电路的数量描述。而在寄存器一级,则可以用寄存器单元中 0 到 1 或者 1 到 0 翻转的位的个数描述,即可以用寄存器中原始操作数和结果之间的汉明距离来计算寄存器由于数据变化而产生的功耗,功耗函数可表示为 $W=H(D\oplus R)$。这里 W 表示模拟的功耗值,H 表示数据的汉明重量,D 和 R 分别表示寄存器变化前后的状态,也就是原始操作数和结果,$H(D\oplus R)$表示 D 和 R 的汉明距离。以异或操作为例,该操作在寄存器中产生的数据变化是 $x\oplus y\rightarrow x$,其中保存变量 x 的目的寄存器可能发生翻转,而保存变量 y 的寄存器并不发生变化。根据汉明距离功耗模型,异或操作在寄存器级的功耗可模拟为 $P_{XOR}=H(x\oplus(x\oplus y))=H(y)$。

4.3 针对 DES 加密算法的差分功率分析仿真

数据加密标准(Data Encryption Standard,DES)利用 64 位密钥,将 64 位明文经过初始置换、16 轮乘积变换、逆初始置换 3 个阶段的运算产生 64 位的密文。其详细算法描述可参见文献[3]。

在攻击 DES 加密算法的第 16 轮子密钥时,一个 S 盒经 2^6 次猜测可得到其中 6 位 K_{16}。D 函数选择一个只与密文和子密钥 K_{16} 相关的函数,D 函数描述如下:

$$D=CTOL_1\oplus SBOX_{n(1)}(K_{16}^{n}\oplus CTOR_{1-6}) \tag{8}$$

其中 D 代表第 15 轮产生的 L_{15} 中的一位,值为 0 或 1;K_{16}^{n} 表示 K_{16} 的第 n 个子密钥块,是要猜测的对象;CTOL 和 CTOR 是根据密文进行反向逆初始置换得到的两个 32 位数据,$CTOL_1$ 是 $CTOL$

中与 D 对应的一位；$CTOR_{1-6}$ 表示 $CTOR$ 中与 K_{16}^{n} 对应进行运算的 6 位；$SBOX_{n(1)}$ 表示第 n 个 S 盒的 4 位输出中的某一位。

假定加密过程用 j 表示，把 DES 第 16 轮运算中 L_{15} 异或 S 盒输出的操作产生功耗的那一时刻记为 j^{*}。在差分功耗分析时，当 $j=j^{*}$ 且 K_{16}^{n} 猜测正确时，D 函数的值与所代表的目标位的值将完全吻合。将 D 为 0 的功耗曲线归入集合 S_0，将 D 为 1 的功耗曲线归入集合 S_1，根据式(7)计算集合 S_0 与 S_1 平均功耗值之差，这时差分功耗曲线上就会出现一个显著的尖峰。当 $j=j^{*}$ 且 K_b 猜测错误时，或当 $j\neq j^{*}$ 时，D 函数与目标位不相关，这时期望，随着样本数增加，差分功耗曲线将变得平滑，不会出现显著的尖峰。

仿真时选择汉明距离模型模拟 FPGA 寄存器级的功耗特征，把 DES 第 16 轮运算中的 L_{15} 与 S 盒输出的异或操作作为功耗测量点，根据第 2 章中描述的 DPA 攻击过程，针对 FPGA 的 DES 加密，实现了 DPA 仿真平台。在 Dell Inspiron(TM) 6400 笔记本电脑(英特尔酷睿 T2050，1.60 GHz 双核处理器，1 GB DDR 内存)上运行仿真程序，在随机明文样本空间为 2 000 的情况下，DPA 仿真攻击的成功率达到 100%，整个攻击耗时不超过 3 min。图 2 为 6 位子密钥猜测正确和错误时仿真结果对比。

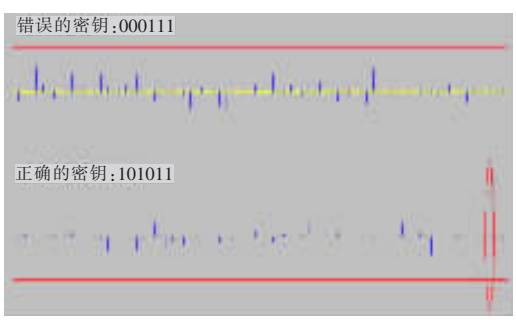

图 2　6 位子密钥 DPA 仿真结果对比

5　结论

本文通过对 SRAM 型 FPGA 的组成结构、功耗产生机理的分析，建立了 FPGA 功耗模型和 DES 加密过程的 DPA 仿真模型，实现了 DPA 仿真平台，并利用仿真平台验证了 FPGA 实现 DES 加密算法对 DPA 的脆弱性。利用这些功耗模型和仿真平台在没有复杂测试设备与测试手段的情况下，可以实现 DPA 仿真攻击，仿真结果同实际的实验结果[6]基本一致，说明 FPGA 功耗模型正确，DPA 仿真能正确反映 DES 加密算法的功耗情况，这对于研究其它加密算法如 AES 等的 DPA 攻击与防护具有很强的借鉴意义。(收稿日期：2007 年 1 月)

参考文献：

[1] Kocher P，Jaffe J，Jun B.Differential power analysis [C]//Wiener M. LNCS 1666：Advances in Cryptology：Proceedings of CRYPTO'99. Santa Barbara，CA，USA：Springer-Verlag，1999：388-397.

[2] Standaert F X，Siddika B.Power analysis attacks against FPGA implementations of the DES [C]//LNCS 3203：Proceedings 14th International Conference on FPL 2004.Leuven，Belgium：Springer，2004：84-94.

[3] Patarin J.Data encryption standard [M].[S.l.]：National Bureau of Standards.U.S.Department of Commerce，1997.

[4] Weste N，Eshraghian K.Principles of CMOS VLSI design[M].U.S.：Addison-Wesley，1993：212-232.

[5] Shang L，Kaviani A S，Bathala K.Dynamic power consumption in Virtex-II FPGA family [C]//Proceedings of the 2002 ACM/SIGDA，10th International Symposiumon Field-Programmable Gate Arrays. U.S.：ACM Press，2002，132：157-164.

[6] Siddika Berna Örs，Elisabeth Oswald，Bart Preneel.Power-analysis attacks on an FPGA-first experimental results [C]//LNCS 2779：Proceedings of CHES 2003，5th International Workshop.Cologne，Germany：Springer-Verlag，2003：35-50.

(上接 86 页)

6　结论

汉字笔段提取对于汉字识别，汉字细化以及汉字字体的自动生成有重要意义，本文以骨架点的半径值分析为着眼点，发现了骨架点半径与毛刺及笔划交叉畸变之间的联系，找到了一种既使骨架保持原图像的连通性，又能消除毛刺和畸变的方法，由此提出了一种行之有效的汉字笔段提取方法。实验结果反映了本方法的准确性和科学性。将该方法用在基于结构模型的手写体汉字识别系统[10]中，取得令人满意的效果。本文中提供的一些参数是人为设定的，下一步的工作是与汉字识别相结合，使系统优化这些参数，从而让识别率进一步提高。
(收稿日期：2007 年 1 月)

参考文献：

[1] Gonzalez R C，Woods R E.Digital image processing[M].2nd ed.Be-Jing：Publishing House of Electronics Industry，2004：420-453.

[2] 曹铁勇，杨吉斌，张雄伟.基于势能平衡的图像骨架抽取算法[J].东南大学学报：自然科学版，2003，33(6)：724-727.

[3] Liu K，Huang Y S，Suen C Y.Identification of fork points on the skeletons of handwritten Chinese characters[J].IEEE Transactions on Pattern Analysis and Machine Intelligence，1999，21(10)：1095-1100.

[4] 张洪波，赵钢，周启龙.图像细化及其连通性保持的方法研究[J].沈阳农业大学学报，2004，35(3)：256-258.

[5] 盛业华，唐宏，杜培军，等.一种保形的快速图象形态细化算法[J].中国图象图形学报，2000，5(2)：89-93.

[6] 吕俊白.一种有效的二值图像细化算法[J].计算机工程，2003，29(18)：147-148.

[7] 孙星明，杨茂江，刘国华.完全基于结构知识的汉字笔画抽取方法[J].计算机研究与发展，2000，37(5)：543-550.

[8] Lee C N，Wu B.Chinese-character-stroke-extraction algorithm based on contour information [J].Pattern Recognition，1998，31(6)：651-663.

[9] 刘峡壁，贾云得.汉字笔段形成规律及其提取方法[J].计算机学报，2004，27(3)：390-395.

[10] 刘峡壁，贾云得.用于手写体汉字识别的汉字结构模型[J].北京理工大学学报，2003，23(3)：322-326.