一种高效功耗攻击物理实验平台研究

李 浪[1,2] 李 静[2] 李仁发[2] 吴克寿[3]
(衡阳师范学院计算机系 衡阳 421008)[1] (湖南大学计算机与通信学院 长沙 410082)[2]
(厦门理工学院计算机系 厦门 361024)[3]

摘 要 功耗攻击是近年来一种对加密芯片密钥攻击最大的威胁,加密芯片功耗攻击与防御成为了研究热点。但功耗分析的实验平台构建却比较困难。以AES加密算法芯片为例,构建了一个基于FPGA的高效功耗攻击物理实验平台。详细叙述了物理实验平台的建立过程、实验结果。该功耗攻击物理实验平台构建相对简单,实验运算速度较快,且具有加密算法易于修正的灵活性,可以方便地对加密算法的功耗特性进行改进与验证。在功耗分析模型上,设计了一种高效功耗攻击模型,该模型在差分统计速度上提高了一个数量级,可为抗功耗攻击研究进行快速实验提供参考。

关键词 功耗分析,AES,物理实验平台,功耗模型
中图法分类号 TP309 **文献标识码** A

Research of an Efficient Power Analysis Physical Experiment Platform

LI Lang[1,2] LI Jing[2] LI Ren-fa[2] WU Ke-shou[3]
(Department of Computer, Hengyang Normal University, Hengyang 421008, China)[1]
(School of Computer and Communication, Hunan University, Changsha 410082, China)[2]
(Department of Computer, Xiamen University of Technology, Xiamen 361024, China)[3]

Abstract Power analysis attack has become a great threat to encryption chips. Attacks and defense of power analysis have become the research hotspot. However, experimental platform of power analysis is more difficult to build for researchers. AES encryption algorithm was used to build a high-performance FPGA-based physical experiment platform for power analysis as an example. The process of establishing the physical experimental platform was described in detail. The platform is relatively simple, fast test speed, flexibility. It will be convenient to verified for the encryption algorithm of the power. The efficient power analysis model was proposed. It can improve the exprimental speed in the differential statistics.

Keywords Power analysis, AES, Physical experiment platform, Power analysis model

1 引言

与传统密码分析手段不同的是,由于加密算法在芯片上实现,加密芯片电路在运行过程中会泄漏一些有用信息,比如运算时间、电磁辐射、功耗等,这些信息能够用来分析加密算法的敏感数据或密钥,这种方法称为旁路攻击(Side Channel Attacks)[1-3]。旁路攻击易于实施且所需代价低,其基本原理适用于各种密码算法的破解,其中利用功耗信息的旁路攻击手段称为功耗攻击。它由 Paul Kocher 等人于 1998 年提出[4],该方法可以以低成本快速、无损地提取出密码芯片中的密钥,这对密码芯片的安全提出了严重挑战。

功耗分析的实验比较复杂,目前没有全自动化系统集成的分析工具。如何构建一个快速、灵活的功耗分析实验平台,一直是专家学者近年来研究的重点。本文以 AES 算法为例,详细说明了如何用硬件描述语言 Verilog HDL,EDA 工具在 FPGA 上建立 AES 芯片原型,并以此建立一个高效功耗分析物理实验平台的完整过程。

2 基于 FPGA 的功耗分析实验平台

FPGA 是现场可编程门阵列,具有体系结构和逻辑单元灵活、集成度高以及适用范围宽等特点,兼容了 PLD 和通用门阵列的优点,可实现较大规模的电路,编程也很灵活。它与门阵列等其它 ASIC 芯片相比,具有开发周期短、设计制造成本低、开发工具先进、标准产品无需测试、质量稳定以及可实时在线检验等优点,因此被广泛应用于产品的原型设计和产品生产之中。几乎所有应用门阵列、PLD 和中小规模通用数字集成电路的场合均可应用 FPGA。

FPGA 的基本特点主要有:

一是采用 FPGA 设计 ASIC 电路,用户不需要投片生产,就能得到合适的原型芯片。

二是 FPGA 可做其它全定制或半定制 ASIC 电路的试样片。

到稿日期:2009-07-20 返修日期:2009-09-24 本文受国家自然科学基金(60903203),湖南省科技计划项目(2009GK3023)资助。
李 浪(1971-),博士,副教授,CCF 高级会员,主要研究方向为嵌入式系统安全,E-mail:lilang911@126.com;李 静(1986-),硕士生,主要研究方向为嵌入式系统安全;李仁发(1957-),教授,博士生导师,主要研究方向为嵌入式计算与安全;吴克寿(1975-),博士,副教授,主要研究方向为嵌入式系统安全与算法设计。

三是 FPGA 是 ASIC 电路中设计周期最短、开发费用最低、风险最小的器件之一。

基于 FPGA 功耗分析实验平台如图 1 所示。

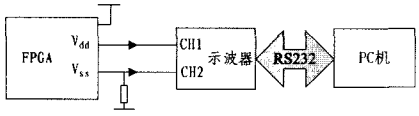

图 1　FPGA 功耗分析实验示意图

下面以 AES 算法为例构建了功耗分析物理实验平台，重点介绍 AES 算法在 FPGA 上的芯片原型实现及各步的仿真验证过程与结果。在后期的 PC 机处理功耗波形上，设计了一种高效功耗模型，其在处理速度上提高了一个数量级。

3　AES 算法的 Verilog HDL 语言实现

硬件描述语言(HDL)是一种用文本形式描述和设计电路的语言。设计者利用 HDL 描述设计，然后用 EDA 工具进行综合和仿真，最后变为某种目标文件，再用 FPGA 来实现。由于其语言标准化，可以很容易将完成的设计移植到不同厂家的不同芯片中。Verilog HDL 的设计具有工艺无关性，使得工程师在功能设计、逻辑验证阶段可以不过多地考虑门级及工艺实现的细节，只需要根据系统设计的要求，施加不同的约束条件即可设计出实际电路。具体设计流程如图 2 所示。

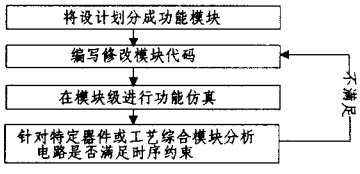

图 2　设计流程

AES 算法(128 位密钥)除最后一个模块外，前 9 圈变换包含的模块相同，而最后一圈除了没有列混合以外，其它变化也与前 9 圈相同，所以将每一个变换单独作为一个模块实现。

3.1　字节替换模块

一个查找表的语句实现如下：

```
always@(state)
case(state)
8'h00:dout=8'h63;
8'h01:dout=8'h7c;
```

实现了一个查找表。s 盒是一个 16 * 16 的矩阵，大小为 256 个字节。用一个一维表实现，例如输入字节 19，查找到第 20 个位置包含的内容为 D4。将状态 19 用 D4 来替换，达到非线性变换的目的。

3.2　列混合

要实现

$$S'_{00}=(02\quad 03\quad 01\quad 01)\begin{pmatrix}S_{00}\\S_{10}\\S_{20}\\S_{30}\end{pmatrix}$$

即

$S'_{00}=\{02\}\cdot S_{00}\oplus\{03\}\cdot S_{10}\oplus\{01\}\cdot S_{20}\oplus\{01\}\cdot S_{30}$

而$\{02\}S_{00}$可以表示为 S_{00} 的移位操作。用 bb[1：8]代替 S_{00}，bb[1]表示 S_{00} 的最高位。判断 S_{00} 最高位是否为 1。若为 1，将 S_{00} 左移一位后异或 1b；若不为 1，仅将 S_{00} 左移一位。

```
assign
out[1：8]=((bb[1]==1)? (bb[1：8]<<1)^8'h1b：
(bb[1：8]<<1))^((bb[9]==1)? (bb[9：16]<<1)^bb
[9：16]^8'h1b：(bb[9：16]<<1)^bb[9：16])^bb[17：24]^
bb[25：32];
```

3.3　密钥扩展

每一轮的密钥都是由前一轮的密钥和本轮密钥共同产生的。

$$w_i=w_{i-4}\oplus Sub(RotByte(w_{i-1}))\oplus Rcon$$

$$w_{i+1}=w_{i-3}\oplus w_i$$

$$w_{i+2}=w_{i-2}\oplus w_{i+1}$$

$$w_{i+3}=w_{i-1}\oplus w_{i+2}$$

密钥变换图如图 3 所示。

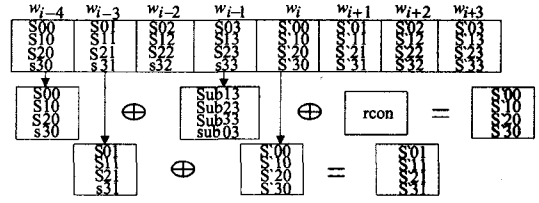

图 3　密钥变换图

3.4　仿真结果

对上述实现进行了仿真，结果如图 4 所示。

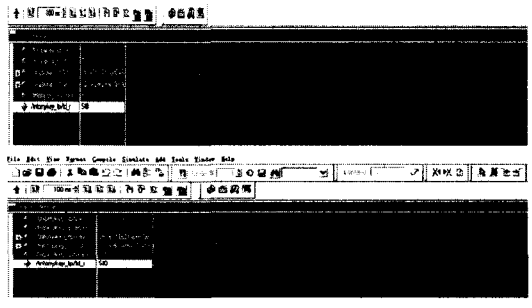

图 4　仿真波形图

3.5　AES 模块

仿真结果如图 5 所示。

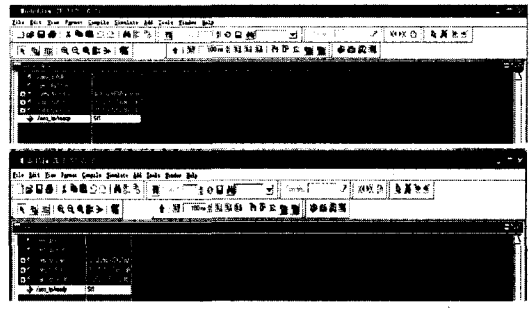

图 5　仿真波形图

部分代码如下：

```
shift s(. aesin(s_box),
    . bb(aa));
mix m(. bb(aa),
    . out(s_mix));
ntomykey nl(. clk(clk),
. reset(reset),
        . key(key),
        . out(ekey),
        . ld_r(ld_r),
        . ready(red));
assign s_add = s_mix ^ ekey;
```

```
always @(posedge clk)
  begin
    counter <= |counter ? counter-4'h1:0;
    s_box <= ld_r ? state^ekey:s_add;
    result <= ready ? result:( |counter ? s_add:aa^ekey );
    ready <= |counter ? 0:1;
  end
```

4 基于 EDK 的 FPGA 系统设计

对于 FPGA 的开发，Xilinx 公司提供了集成开发环境 ISE，支持 VHDL 和 Verilog HDL 及电路原理图。使用 FPGA 设计加密芯片的最大优势在于定制性。

4.1 基本设计流程

EDK 包含了所有用于设计嵌入式编程系统的集成开发解决方案，包括 XPS 工具及嵌入式 IBM PowerPC 硬件处理器核、XILINX MicroBlaze 软处理器核及设计所需技术文档和 IP。Platform Studio 是用于嵌入式处理设计的平台，本文设计使用 EDK 9.1i 版本。图 6 为基本设计流程示意图。

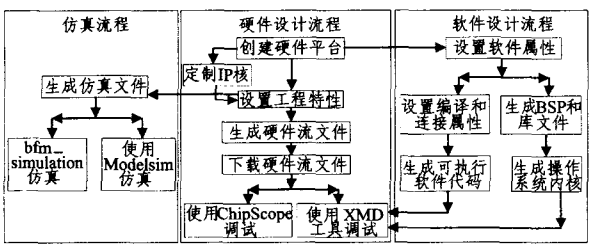

图 6 基本设计流程

4.2 FPGA 实现过程

将 shbox.v 文件复制到 pores 文件夹下，并在 pao 文件中声明。

在 user_logic 文件中添加声明语句：

```
//--user logic implemention added here
Assign state=slv_reg0
Shbox mybox (.state(state),.dout(dout);
//------------
//implement slave model register(s)
Always @(posedge Bus2Ip_clk)
Begin:SLAVE_REG_WRITE_PROC
  Slv_reg1<=dout;
```

将每个模块单独下载成功后，开始下载完整 IP 核。硬件部分成功下载网表和比特流后，修改软件程序：在“self test.c”文件中添加主函数。系统配置时点选添加中断。在 IP 核的设定中，点选 User Logic Interrupt Support，使得用户逻辑可以通过总线发出中断请求。User Logic S/W Register Support，用户逻辑含有软件可以寻址和访问的寄存器。最终下载结果如图 7 所示。

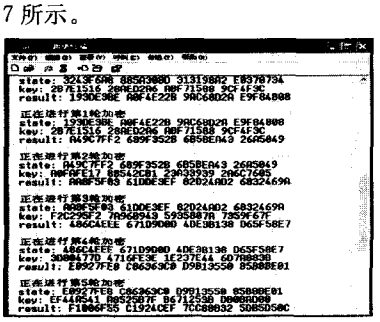

图 7 仿真结果

5 高效功耗分析模型与实验

上面详细描述了 AES 算法的原型芯片在 FPGA 上的实现过程，本节在上述基础上描述基于 FPGA 的功耗分析实验平台的建立。

门电路的主要功耗来自动态功耗，信号有 4 种变化状态：0→1，0→0，1→0，1→1，其中状态从 0→1，1→1 时，由于没有负载电容充放电过程，几乎没有功耗；而从 1→0 时，电场能置换为热能；只有从 0→1 时，电源端才有功耗。对于单个的门电路，用汉明重量建立功耗模型，要考虑从 1 到 1 变化的功耗。由于充放电时，寄存器从 1 到 1，几乎不产生功耗；用汉明距离建立功耗模型，则要考虑从 1 到 0 变化的功耗；从 1 到 0 翻转时，主要产生的是热能，不会对功耗产生影响。因此，本文只考虑寄存器从 0 到 1 翻转时产生功耗的功耗模型：

$$W=aH(D_0\rightarrow R_1)+b \tag{1}$$

式中，W 为功耗，D 和 R 分别为寄存器前一状态和当前状态的值，b 为由噪声和其他与输入信号无关变量引起的功耗，a 为常数，$H(D_0\rightarrow R_1)$ 代表前一状态中为 0 的位与对应当前状态中为 1 的位的个数。

实验表明，在功耗分析物理实验平台中采用此种简化功耗模型并不影响实验结果的正确性。图 8 为对未加防护（即本文前面实现）的 AES 算法选用 5000 条明文攻击成功的结果图。正是由于采用了简化的高效功耗分析模型，攻击实验速度在同类实验中是比较快的。

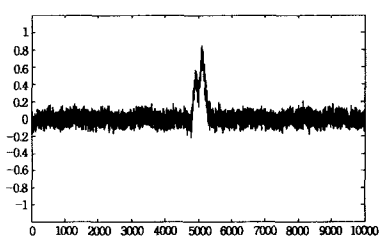

图 8 物理攻击结果示意图

结束语 功耗攻击物理实验过程目前仍然比较复杂，传统的综合、提取网表等实验时间也很长，而且一旦发现加密算法设计有问题，得重新设计，耗时较多。本文利用 FPGA 能够快速形成加密算法芯片原型的特点，对功耗分析的物理实验平台建立进行了详细构建。该功耗分析物理实验平台能够给功耗分析学者们提供一个较好的物理实验思路和参考。

参 考 文 献

[1] Kocher P, Lee R, et al. Security as a New Dimension in Embedded System Design[C]// DAC 2004. San Diego, California, USA, 2004: 753-760

[2] Bucci M, Giancane L, Luzzi R, et al. Enhancing power analysis attacks against cryptographic devices[J]. IET on Circuits, Devices & Systems, 2008, 2(3): 298-305

[3] 李浪，李仁发，Edwin H-M S. 安全 SOC 抗功耗分析攻击研究综述[J]. 计算机科学，2009，36(6)：16-18

[4] Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]// Proceedings of Advances in Cryptology-CRYPTO'99. Santa, Barbara, CA, USA, 1999: 388-397