基于 AT89C51 物理功耗攻击实验平台研究*

李 浪[1,2]，李肯立[2]，焦 铬[1]，王玉奇[1]，邹 祎[1]
(1. 衡阳师范学院 计算机科学系，湖南 衡阳 421002；2. 湖南大学 数学博士后流动站，长沙 410082)

摘 要：功耗攻击是一种对加密芯片密钥进行攻击的方式，加密芯片功耗攻击与防御是目前信息安全的研究热点。但功耗分析的实验平台构建却比较困难，以 DES 加密算法为例，构建了一个基于 AT89C51 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、注意事项、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。

关键词：功耗攻击；DES；AT89C51；物理实验平台
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2012)07-2681-02
doi:10.3969/j.issn.1001-3695.2012.07.076

Research of power analysis physical experiment platform based AT89C51

LI Lang[1,2], LI Ken-li[2], JIAO Ge[1], WANG Yu-qi[1], ZOU Yi[1]
(1. *Dept. of Computer Science, Hengyang Normal University, Hengyang Hunan* 421002, *China*; 2. *Mathematical Postdoctoral Research Station, Hunan University, Changsha* 410082, *China*)

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. This paper used DES encryption algorithm to build a high-performance AT89C51-based physical experiment platform for power analysis as an example, and described the process of establishing the physical experimental platform in detail. The platform is relatively simple , fast test speed, flexibility. It will be convenient to verified for the encryption algorithm of the power analysis attacks.

Key words: power analysis attack; DES; AT89C51; physical experiment platform

0 引言

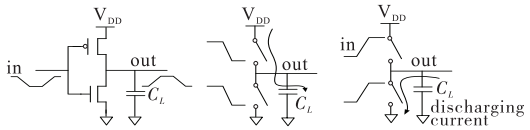
旁路攻击是一种新型的密码破解方式，与传统密码分析手段不同，它是利用加密芯片在运行过程中泄漏功耗、电磁辐射、运算时间等信息，通过这些信息分析加密算法密钥[1~3]。旁路攻击易于实施且所需代价低，其基本原理适用于各种密码算法的破解，其中利用功耗信息的旁路攻击称为功耗攻击。它由 Kocher 等人[4]于 1998 年提出，该方法可以低成本、快速、无损地提取出密码芯片中的密钥。

本文以 DES 算法为例，详细说明了在 AT89C51 单片机上构建一个高效功耗分析物理实验平台的完整过程。

1 基于 AT89C51 的功耗攻击物理平台结构

1.1 基本原理

CMOS 反相器通过监测系统引脚上的电流或电压等物理泄漏信息来获取密码芯片密钥，如图 1 所示，电路的功耗是同一时刻所有改变状态的门电路功耗之和，电路中改变状态的门越多，相应功耗也就越大。电路功耗的测量可以通过在加密芯片的电源引脚 V_{DD}(或接地引脚 V_{ss})和真实电源 +5V 端(或电源接地端 GND)之间串联一个适当电阻(串联电阻的目的是为了放大测量电压信号)，并对其电压进行测量来实现。数字电路的功耗分为静态功耗和动态功耗，CMOS 数字电路在以高速时钟频率工作时，其静态功耗相对于动态功耗来说是可以忽略不计的。



(a) CMOS反相器 (b) 充电电流 (c) 放电电流

图 1 CMOS 反相器

1.2 基于 AT89C51 物理功耗攻击实验平台

实验平台构建示意图如图 2 所示。

由 PC 机产生随机明文，经串口下载到加密电路板，示波器记录下电阻 R 上的瞬时电压，送回 PC 机作统计信号分析。由图 2 可知，真实功耗数据采集需要关注三大模块：加密测试

收稿日期：2011-12-25；**修回日期**：2012-01-31 **基金项目**：国家自然科学基金资助项目(61133005)；湖南省教育厅青年项目(11B018)；衡阳师范学院科学基金资助项目(11B43)；湖南省重点建设学科(光学)资助项目；湖南省博士后基金资助项目(897203005)

作者简介：李浪(1971-)，男，湖南衡阳人，副教授，博士，主要研究方向为嵌入式安全(lilang911@126.com)；李肯立(1971-)，教授，博导，主要研究方向为高性能计算与信息安全；焦铬(1979-)，男，湖南湘阴人，讲师，硕士，主要研究方向为嵌入式计算；王玉奇(1974-)，男，讲师，主要研究方向为信息安全；邹祎(1983-)，女，湖南衡阳人，讲师，硕士，主要研究方向为嵌入式计算.

模块、示波器采集模块和 PC 机数据处理模块。

图 2 物理功耗攻击实验平台示意图

1.3 加密测试模块

加密电路板由两部分构成,接口负责数据格式转换和握手信号产生。数据格式转换是指由 PC 机经串口或并口传送过来的随机明文输入矢量转换为加密算法实现能够接受的字节格式。握手信号则是每次加密运算需要明文载入、密钥载入、加密启动和加密结束等。此外,接口还需要产生触发信号,控制示波器只记录功耗攻击分析中感兴趣的采样点。

1.4 示波器采集模块

示波器通过 RS-232 与 PC 机互连,在 DPA 实验中采用以太网实现示波器控制和波形数据传输。一般以通道 1 记录电阻上的电压信号作为加密电路的瞬时功耗,通道 2 记录触发信号,得到的波形数据以文本文件形式保存。文件数据结构包括分隔符、信号名称、信号数值、时间标度等,根据触发信号可以把与加密运算相关的功耗数据提取出来。

1.5 PC 数据处理模块

得到功耗数据后,为了消除测量噪声干扰和减少统计分析运算量,需要对波形数据进行预处理。这通常包括数据同步、均值滤波两个步骤。数据同步保证每次加密运算过程所测量的功耗曲线采样点严格对齐,实验中是通过每次加密运算的触发信号实现的。均值滤波包括对同一明文重复加密的功耗曲线求平均值,以及功耗曲线内多个连续采样点求平均值。最终得到的功耗曲线数据,可以进行统计分析,可以用 C 编程或 MATLAB 进行数据处理。

2 物理实验平台实例构建

把加密算法以及改进的加密算法通过相应的工具及其软件导入到 AT89C51 单片机上,在导入时,由于 AT89C51 存储空间有限,必需要对 DES 加密算法作优化才能完全写入。

图 3 是实物实验过程示意图,其中示波器外接的 U 盘用于保存指定功耗数据,可以用于后期处理和功耗统计分析。

图 4 所示为从互联网上下载的共享软件,用于同单片机进行通信、发送加密数据。

图 5、6 为单片机 AT89C51 的接口及探头连接示意图。

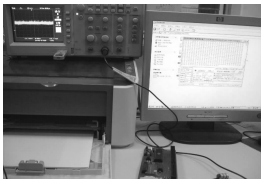


图3 AT89C51实验示意图

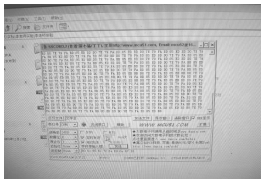


图4 串口通信

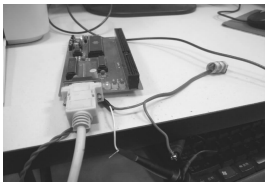


图5 接口示意图

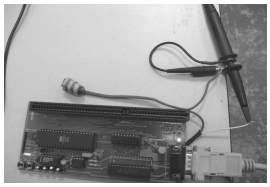


图6 探头的连接

图 7 为单片机 AT89C51 的 PCB 板的背面图,由于 PCB 板上有电容等其他干扰元器件,直接从单片机接地引脚引了一根线出来,这样就保证了信号测量的准确性。

图 8 为 PCB 背面放大图,可以清晰地看到直接引出的 AT89C51 接地端,从而减少其他无关电路元件对信号的干扰。

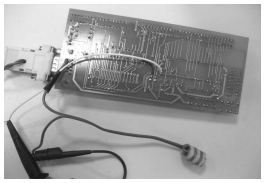


图7 PCB板背面图

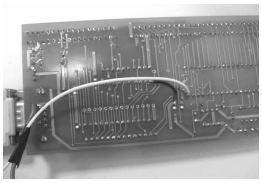


图8 放大后的PCB板背面图

3 实验结果

图 9 为对未加防护的 DES 加密算法测量的波形图,保存在 U 盘上。此图为 U 盘直接拷贝屏幕的结果。

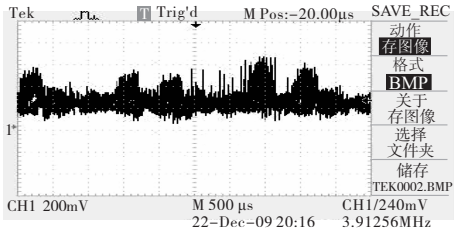


图 9 示波器测量截图

从图 9 中可以看出,未加防护的 DES 加密算法在加密运算时功耗波形差异明显。在后续的数据统计过程中可以利用文献[5]的高效功耗攻击模型进行计算,能够节省功耗攻击分析时间的 3/4。

4 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、提取网表等实验的时间也很长,而且一旦发现加密算法设计有问题,则必须重新设计,耗时较多。本文利用 AT89C51 的经济性,和能够快速形成加密算法芯片物理实验平台的特点,对功耗攻击的 AT89C51 物理实验平台建立进行了详细构建,特别提到了在具体构建过程中的一些注意事项和关键技术。该功耗攻击物理实验平台能够给功耗攻击学者们提供一个较好的物理实验思路和参考。

参考文献:

[1] RAVI S, KOCHER P C, LEE R B, *et al*. Security as a new dimension in embedded system design[C]//Proc of the 41st Design Automation Conference. New York: ACM, 2004: 753-760.

[2] BUCCI M, GIANCANE L, LUZZI R, *et al*. Enhancing power analysis attacks against cryptographic devices [C]//Proc of International Symposium and Systems. 2006.

[3] 李浪, 李仁发, SHA E H M. 安全 SOC 抗功耗攻击研究综述[J]. 计算机科学, 2009, 36(6): 16-18, 25.

[4] KOCHER P C, JAFFE J, JUN B. Differential power analysis[C]// Proc of the 19th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1999: 388-397.

[5] 李浪, 李仁发, 徐雨明, 等. 功耗攻击实验中一种高效功耗模型研究与应用[J]. 计算机应用研究, 2009, 26(12): 4722-4723, 4727.