针对DES加密算法的DPA攻击仿真平台

吴克寿[1] 李仁发[1,2] 王晓栋[1] 陈玉明[1]
(厦门理工学院计算机科学与技术系 厦门 361024)[1] (湖南大学计算机与通信学院 长沙 410082)[2]

摘 要 研究分析数据加密算法DES的特点,采用差分功耗分析(DPA)攻击方式进行密钥破解,针对DES算法实现一种差分功耗分析攻击仿真平台。该仿真平台具有精度高、模拟速度快等特点,其理论基础为集成电路中门电路在实现加密算法时的物理特性、功耗模型及数据功耗相关性。在该平台上针对DES加密系统,采用基于汉明距离的差分功耗攻击实现仿真模拟,成功破解了DES加密算法的密钥,从而给DES加密算法理论研究者提供了有益的基础和参考。

关键词 DES,差分功耗攻击,汉明距离,仿真平台
中图法分类号 TP309 **文献标识码** A

Simulation Platform for Differential Power Analysis Attack on DES

WU Ke-shou[1] LI Ren-fa[1,2] WANG Xiao-dong[1] CHEN Yu-ming[1]
(Department of Computer Science, Xiamen University of Technology, Xiamen 361024, China)[1]
(School of Computer and Communication, Hunan University, Changsha 410082, China)[2]

Abstract By analyzing the features of data encryption algorithm DES, this paper presented a differential power analysis (DPA) attacking simulation platform on DES. The platform has some advances such as high precision and high simulation speed. All its theories are based upon the physical characters, power consumption models and data dependent power consumption of CMOS logic gates which form the integrated circuits(ICs). The paper introduced the design and realization of DPA attacking platform of DES, which is based on hamming distance. Correct secret key of encryption algorithm is cracked successfully with simulation experiment. The work in this article provides necessary base and reference for theoretic research on DES algorithm in the future.

Keywords DES, Differential power analysis attacks, Hamming distance, Simulation platform

1 概述

随着智能卡和计算机网络的迅速发展与不断普及,信息安全问题日益突出,因此各种形式的专用密码电路和密码算法处理器被广泛地应用于各类产品中。目前,常用的密码算法大致可以分为两类:以DES、AES(高级加密标准)为代表的对称算法和以RSA、ECC为代表的非对称算法。DES是目前使用非常广泛的数据加密算法,它于1977年被美国国家标准局作为第46号联邦信息处理标准而采用[1]。

传统的密码破解方法是一种数学攻击手段,通过大量的数学计算来搜索密码系统的密钥。该类攻击方法的一个直接例子就是暴力攻击:穷举所有可能的密钥,直至找到正确的密钥。1999年1月,Deep Crack和distributed.net合作,在22小时15分钟内成功破解了一个DES密钥。虽然暴力攻击能在较短的时间内破解DES密钥,但是仍需要耗费大量的人力和物力,而且如果密钥的长度增加,攻击难度和时间则会急剧增加。近年来出现了一种新的攻击方法:差分功耗分析(DPA)攻击[2]。与其他攻击方法相比较,差分功耗分析攻击具有分析方法简单、密钥搜索空间小等优点。因此,差分功耗分析攻击及防护对策研究受到国内外相关领域的研究人员和业界的极大关注[3-5]。

对DES密码芯片进行差分功耗分析攻击通常需要一套昂贵的系统设备,在芯片正常工作条件下多次实时采集芯片的功耗数据,采样频率通常应当高于工作频率一个数量级以上,然后统计分析海量的数据,提取出密钥等关键数据。这个条件对于许多从事差分功耗分析攻击研究的单位是困难的。因此,本文针对DES算法建立一种差分功耗分析攻击仿真平台,提供一种快速而低成本的密码攻击验证方法,从而给DES加密算法理论研究者提供了有益的基础和参考。

2 DPA攻击原理

目前,集成电路大都采用静态单轨的标准单元实现,其功耗与输入和输出的翻转状态密切相关。下面以反相器为例来分析功耗特性,如图1所示。

文献[6]中单个CMOS门电路功耗模型表示为

$$P_D = C_L V_{DD}^2 P_{0\to1} f$$

式中,f 代表输入发生变化的最大可能速率,即时钟频率;$P_{0\to1}$是时钟变化时在该门的输出端引起 $P_{0\to1}$(即消耗功率)

到稿日期:2011-03-28 返修日期:2011-06-25 本文受国家自然科学基金(60903203)资助。
吴克寿(1975—),男,博士,副教授,主要研究方向为网络信息安全、密码学理论,E-mail:kswu@xmut.edu.cn。

变化事件的概率；C_L 为等效电容，代表了每时钟周期发生开关的平均电容。

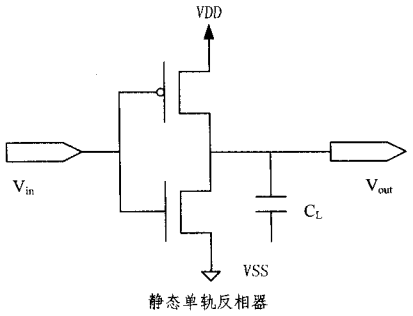

图 1　反相器电路示意图

当输出信号发生 0→1 跳变时，反相器的功耗明显大于发生其它 3 种跳变时的功耗，因此功耗与密码模块中运算的数据具有一定的相关性。功耗分析的原理正是基于这种相关性，攻击者通过统计大量功耗样本即可分析密钥的值。

差分功耗分析(DPA)攻击是一种对密码芯片的泄漏功耗进行统计分析而恢复密钥的攻击方法。DPA 攻击的方法是对大量的曲线样点进行功耗统计测试，即根据大量功耗样本来分析密钥的值，它具有比简单功耗攻击更高的强度。

3　针对 DES 加密算法的 DPA 攻击仿真平台

3.1　基于汉明距离的 DES 加密算法功耗模型

加密芯片在运行 DES 加密程序时，在数据处理过程中，系统中数据的变化在集成电路中表现为功耗的变化。对于系统中参与数据处理的某一寄存器中的一位触发器而言，功耗的大小与所处理的数据是直接相关的。这种关系在门电路一级表现为负载电容充、放电，在寄存器一级表现为寄存器中触发器的 0、1 翻转。在信息论中，两个等长二进制串之间的汉明距离是两个二进制串对应位置的不同字符的个数。因此，可以用汉明距离来表示指令执行前后数据的 0、1 翻转，进而可以模拟加密系统芯片中数据处理过程的功耗情况。

根据寄存器状态的前后变化来建立汉明距离功耗模型，将寄存器单元中的 0、1 翻转与功耗对应起来。寄存器的功耗函数可表示为：

$$W=\alpha H(D\rightarrow R)+\beta$$

式中，W 表示功耗，H 表示数据的汉明距离，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。$H(D\rightarrow R)$表示 D 和 R 的汉明距离，α 和 β 是两个常量参数。令 $\alpha=1$，$\beta=0$，上述模型就可简化为 $W=H(D\rightarrow R)$。

3.2　DES 加密算法 DPA 攻击过程

DES 加密算法的 DPA 攻击过程设计如下。

步骤 1　首先由 DES 加密芯片进行 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) 离散采样第 i 次密码运算产生的功耗，形成的功耗数组为 $S_i[j]$(对应于功耗曲线)，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 $CT_i(0\leqslant i\leqslant N)$。

步骤 2　定义一个与密钥密切相关的分割函数 $D(CT_i, K_b)$。猜测令 $K_b=0$，将基于采样时间点 j 的功耗曲线 $S_i[j]$ 分成两个子集合：

$$S_0=\{S_i[j]\mid D=0,1\leqslant i\leqslant N\}$$

$$S_1=\{S_i[j]\mid D=1,1\leqslant i\leqslant N\}$$

步骤 3　计算集合 S_0 与 S_1 平均功耗值：

$$A_0[j]=\frac{1}{|S_0|}\sum_{S_i[j]\in S_0}S_i[j]$$

$$A_1[j]=\frac{1}{|S_1|}\sum_{S_i[j]\in S_1}S_i[j]$$

从而得到差分功耗曲线：

$$T[j]=A_0[j]-A_1[j]$$

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，转步骤 2，并修改猜测，令 $K_b=K_b+1(K_b<2^6)$，循环运行直到 K_b 猜测正确。

步骤 5　当获取 DES 第 16 轮子密钥 K_b 后，根据 DES 子密钥生成算法，可逆推获取 56 位有效密钥 K 中的 48 位。K 中剩余的 8 位密钥可通过 2^8 次穷举搜索获得。

3.3　DES 加密算法 DPA 攻击仿真平台

示波器是功耗数据采集的有力工具，但价格昂贵，因此，建立了仿真平台来模拟实现功耗采样和功耗分析，如图 2 所示。仿真平台的工作流程如下。

首先，将密码算法用硬件描述语言描述成代码，经代码仿真器验证其正确后，经过逻辑仿真器综合成门级网表，通过网表转换工具转换成晶体管级网表，以便电路模拟器仿真；然后，激励向量生成器产生的激励向量与晶体管级网表合成电路模拟文件，经电路模拟器仿真，并处理模拟结果得到功耗曲线；经过多组激励向量的输入而得到功耗曲线族，送到功耗分析工具，进行差分功耗分析，分析出密钥等关键数据。

该平台的核心包括两个部分：电路模拟器和功耗分析工具。电路模拟器是用来获得芯片电路工作时的功耗曲线，相当于对实际芯片的功耗采样。功耗分析工具则用来完成功耗分析，并进行密钥破解。

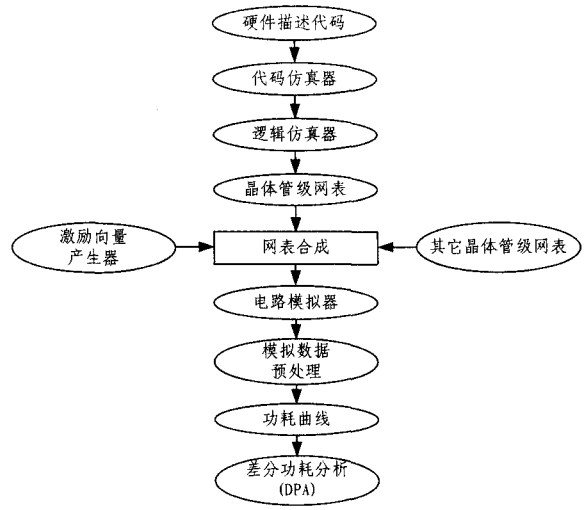

图 2　DPA 攻击仿真平台

4　针对 DES 加密算法的 DPA 攻击实验

本文设计了一个软件模拟的 DPA 攻击的仿真实验平台。下面通过对 DES 加密算法进行功耗模拟，提取出功耗曲线，进行功耗分析。另一方面，亦可以利用这一平台验证抗 DPA 攻击算法设计的有效性。针对 DES 算法的 DPA 攻击仿真实

(下转第 65 页)

结束语 为了实现大幅面多光谱遥感图像配准的批量处理，提出了一种快速自动配准算法。该方法利用图像灰度值、信息熵及特征分布均匀性准则从二级规则网格中选取特征网格，然后采用 SIFT 算法在筛选获取的特征网格中并行地提取特征点，从而减少了运算时间。在特征匹配步骤，改进了原算法的匹配方法，提出了基于位置约束的快速初匹配方法，并利用相关性原理及特征点之间的空间距离约束关系进一步剔除了误匹配，提高了特征匹配准确度。实验结果表明，本文方法能够实现大幅面遥感图像的快速、自动、亚像素级配准。

参 考 文 献

[1] Zitova B, Flusser J. Image registration methods: a survey[J]. Image and Vision Computing, 2003, 21(11): 977-1000

[2] Kern J P, Pattichis M S. Robust Multispectral Image Registration Using Mutual-Information Models[J]. IEEE Transaction on Geoscience and Remote Sensing, 2007, 45(5): 1494-1505

[3] Anthony A, Loffeld O. Image Registration Using a Combination of Mutual Information and Spatial Information[C]// IEEE International Conference on Geoscience and Remote Sensing Symposium. Colorado, U. S. A, 2006: 4012-4016

[4] Yu Le, Zhang Deng-rong, Holden E-J. A Fast and Fully Automatic Registration Approach Based on Point[J]. Computers & Geosciences, 2008, 34(7): 838-848

[5] Zhang Jun. A Study on Automated Image Registration Based on Straight Line Features[J]. 2009 Urban Remote Sensing Joint Event, 2009: 1-6

[6] Eastman R D, Moigne J L, Netanyahu N S. Research issues in image registration for remote sensing[C]// IEEE Conference on Computer Vision and Pattern Recognition. Minneapolis, MN, USA, 2007: 1-8

[7] Wen Gong-jian, Lv Jin-jian, Yu Wen-xian. A High-Performance Feature-Matching Method for Image Registration by Combining Spatial and Similarity Information[J]. IEEE Transactions on Geoscience and Remote Sensing, 2008, 46(4): 1266-1277

[8] Lin Hui, Du Pei-jun, Zhao Wei-chang, et al. Huasheng Sun. Image Registration Based on Corner Detection And Affine Transformation[C]// 3rd International Congress on Image and Signal Processing(CISP). 2010, 5: 2184-2188

[9] 夏德深，傅德胜. 计算机图像处理及应用[M]. 南京：东南大学出版社，2004

[10] Lowe D G. Distinctive image features from scale2invariant keypoints[J]. International Journal of Computer Vision, 2004, 60(2): 91-110

[11] 李志华，陈耀武. 基于多摄像头的目标连续跟踪[J]. 电子测量与仪器学报，2009，23(2)：46-51

[12] 乔警卫，胡少兴. 三维重建中特征点提取与匹配算法研究[J]. 系统仿真学报，2008，20：400-403

[13] 李云霞，曾毅，钟瑞艳，等. 基于 SIFT 特征匹配的图像拼接算法[J]. 计算机技术与发展，2009，19(1)：43-52

[14] 胡明昊，任明武，杨静宇. 一种快速实用的特征点匹配算法[J]. 计算机工程，2004，30(9)：31-33

[15] 张迁，刘政凯，庞彦伟，等. 基于 SUSAN 算法的航空影像的自动配准[J]. 测绘学报，2003，32(3)：245-250

[16] 刘贵喜，刘冬梅，刘凤鹏，等. 一种稳健的特征点配准算法[J]. 光学学报，2008，28(3)：454-461

[17] 中国资源卫星应用中心[EB/OL]. http://www.cresda.com/cn/. 2011.6

(上接第 60 页)

验平台的具体步骤如下。

1) 完成硬件描述语言(如 Verilog, VHDL 等语言)对 DES 加密算法的描述，并编写合适的测试激励函数。

2) 经 Modelsim 逻辑仿真，验证正确后，在相应测试点设置测试激励函数，生成所关心信号量的 VCD(Value Change Dump)文件。VCD 文件实质上是记录了相应时间测试点功耗波形的二进制形式的文件。

3) 通过 Visual C++语言编程处理 VCD 文件，描绘出 DES 加密算法功耗攻击波形曲线。

4) 采用 DPA 攻击方法和穷举法得到 DES 加密算法的密钥。

图 3 所示的是 DES 加密算法在 3000 条明文下对第一轮的子密钥进行 DPA 攻击成功的波形。

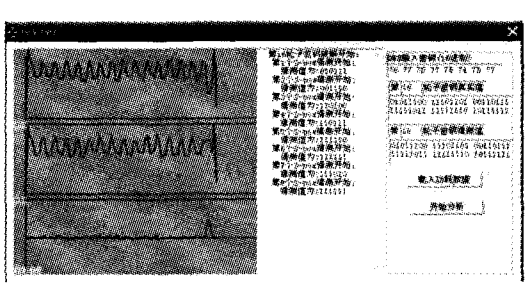

图 3 DPA 攻击成功

结束语 差分功耗分析(DPA)攻击不同于常规的针对加密算法的穷举攻击策略，其原理设计巧妙，攻击设备虽贵但易于软件仿真实现。本文建立了 DES 加密过程的 DPA 攻击仿真平台，利用该仿真平台，在没有复杂测试设备与测试手段的情况下分析了 DES 加密算法在面临 DPA 攻击时的脆弱性，从而为 DES 算法的理论研究与设计工作者提供了有益的参考价值。

参 考 文 献

[1] Data Encryption Standard. Federal Information Processing Standard(FIPS) Publication 46, National Bureau of Standards[S]. US Department of Commerce, Washington DC, 1977

[2] Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]// Proceedings of Advances in Cryptology-CRYPTO99. Springer-Verlag, 1999: 388-397

[3] Alioto M, Poli M. A general model for differential power analysis attacks to static logic circuit s[C]// PPISCAS 2008. Piscataway, NJ: IEEE, 2008: 3346-3349

[4] 李浪，李仁发，童元满，等. 嵌入式加密芯片功耗分析攻击与防御研究进展[J]. 计算机研究与发展，2010，47(4)：595-604

[5] 陈开颜，赵强，褚杰，等. 差分功耗分析单片机 DES 加密实现的旁路攻击[J]. 计算机科学，2007，34(11)：20-22

[6] Rabaey J M. Digital Integrated Circuits[M]. Englewood Cliffs, NJ: Prentice-Hall, 1996