差分功耗分析单片机 DES 加密实现的旁路攻击*)

陈开颜 赵 强 褚 杰 邓高明
(军械工程学院计算机工程系 石家庄 050003)

摘 要 在研究 DPA 的原理和方法、分析 CMOS 芯片工作时功率消耗原理的基础上,完成了对 DES 加密算法的 DPA 攻击的仿真实现,并对运行在 AT89C52 单片机上的 DES 加密程序进行 DPA 攻击实验,在 10^6 个明文样本的条件下,成功获得了 DES 第 16 轮加密的 48 位密钥。在验证仿真方法正确性的同时进一步证明了 DES 加密实现面对 DPA 攻击的脆弱性。

关键词 旁路分析(侧信道分析),差分功耗分析,DES

Side-channel Attacks on Single-chip DES Implementation Using Differential Power Analysis

CHEN Kai-Yan ZHAO Qiang CHU Jie DENG Gao-Ming
(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003)

Abstract Based on the principle of DPA and power leakage principle and leakage model of CMOS device, we first complete software simulation experiment, then we implement DPA attacks to DES running on AT89C52. We succeeded to receive 48-bit key of 16-th round at 10^6 power samples. This verifies our simulation method and vulnerability of DES implementation for DPA attacks.

Keywords Side-channel cryptanalysis, DPA, DES

1 引言

一个密码要素包括建立与实现两个方面。从建立方面,可以将它看作一个数学对象的抽象,如在一个密钥的作用下,通过某种变换将某一输入转换成另一输出;从实现方面看,这个要素最终将在特定的硬件和特定环境下的程序中执行,因此将呈现出特殊的执行特征。

传统的建立在数学分析基础上的密码分析学主要针对的是数学抽象。它一般在纯算法的层面上进行研究,力求找出算法或协议设计上的缺陷。由于密码算法或协议的数学安全性基础比较牢固,因此在进行数学分析时非常困难。

旁路攻击(Side Channel Attacks,简称 SCAs)技术避开了对密码算法进行繁琐的数学分析,而研究算法在具体实现时呈现出的特殊的特征信息。它是一种新型密码分析技术,它通过监控密码设备在进行密码运算期间所呈现的功耗、电磁辐射、运行时间等物理特征信息,结合数学分析的方法,从中萃取出与密码运算相关的信息,并进一步获取运算中涉及到的秘密参量。图 1 为旁路攻击环境下的密码系统。实践证明,这种将密码算法与算法的具体实现相结合进行分析攻击的方法在许多场合下更为有效。

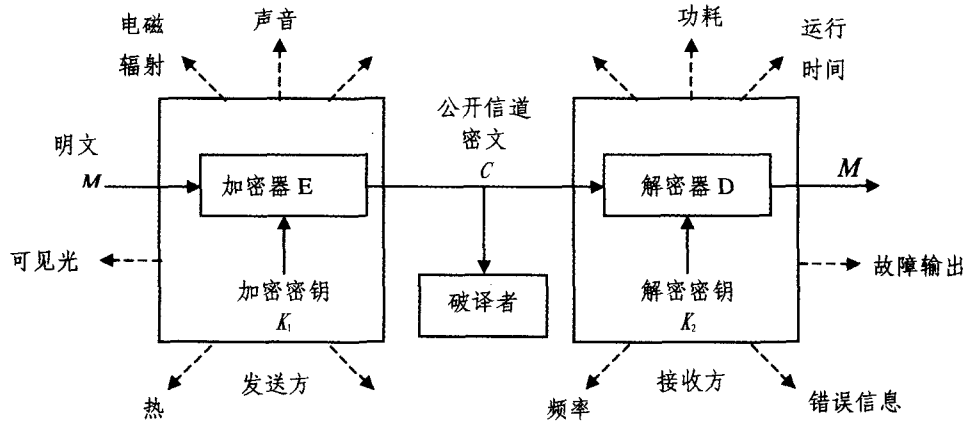

图 1 旁路攻击环境下的密码系统

迄今为止,在所有已知的旁路攻击技术当中,功耗分析攻击是研究得最为广泛并且得到实验验证的一种。功耗分析攻击(power analysis attacks)是通过分析密码设备进行操作的功率消耗,来推导出加密系统所进行的操作和在操作中涉及到的秘密参量。通常根据对功率消耗的不同分析方法,Kocher 等人介绍了简单功耗分析(simple power analysis,简称 SPA)和差分功耗分析(differential power analysis,简称 DPA)[1]。T. S. Messerges[2]和 B. den Boer[3]描述了利用功

*)本课题得到国家自然科学基金(60571037)、军械工程学院科学研究基金(YJJXM630)资助。陈开颜 博士生,副教授。

耗分析进行实际攻击的结果。Akkar 等人[4]给出由指令、操作数等产生的功耗泄漏值，并提出了一个泄漏模型。Th. S. Messerges[5]提出了一个改进的功耗分析。Chari 等人[6]提出一个新的功耗分析攻击的方法，称为模板攻击。

本文在研究了 DPA 的原理和方法、分析 CMOS 芯片工作时功率消耗原理的基础上，完成了对 DES 加密算法的 DPA 攻击的仿真实现；在 10^3 个明文样本条件下，成功获得了 DES 第 16 轮加密的 48 位密钥，之后对运行在 AT89C52 单片机上的 DES 加密程序进行 DPA 攻击实验；在 10^6 个明文样本的条件下，成功获得了 DES 第 16 轮加密的 48 位密钥。

本文第 2 部分介绍了 DPA 的原理和方法，第 3 和第 4 部分分别给出了 DPA 攻击的仿真及实验结果。最后分析实验结果以及今后的研究方向。

2 差分功耗分析攻击概述

当前先进的电子设备采用超大规模集成电路(VLSI)设计，而 VLSI 中占统治地位的是数字 CMOS 逻辑电路[7]。CMOS 门电路的主要功耗来自动态功耗，即 COMS 门电路充放电(0→1、1→0、0→0、1→1)产生的功耗，通常称其为汉明距离泄漏(hamming distance leakage)功耗[8]。

功耗分析攻击利用密码设备在进行密码运算时产生的功耗信息，来推导出运算中的秘密参量。功耗分析攻击的基本假设包括：

1)攻击者了解并且能够控制密码算法的明文输入，并且需要知道明文或密文。

2)设备的功率消耗必须依赖于被处理的数据。

3)对于所有不同的明文和密钥来说，密码算法的执行时间是一个常数。并且对于相同的明文和密钥来说，重复算法执行所呈现的功率消耗特性应该完全相同。

4)实验测量获得的所有波形没有失真，或者失真在分析允许的范围之内。

5)重复试验并对结果进行平均化处理可以减少密码设备、环境和测量装备所产生的噪声。

按照分析方法之不同，功耗分析可分为简单功耗分析(simple power analysis，简称 SPA)和差分功耗分析(differencial power analysis，简称 DPA)两种。SPA 利用加密操作实现细节与功耗之间的关系，直接从一次测量的功耗轨迹获取密钥信息。我们主要研究 DPA 攻击，它是在分析过程中利用统计学方法，考虑秘密参量和功率消耗之间精细的统计相关性。

比较有效的统计分析方法有均差测试(distance-of-mean test)以及相关性分析(correlation analysis)。本文使用均差测试方法。在均差测试中，我们用 H 表示加密操作过程中的中间预测值。对于一组足够数量的功耗采样轨迹，通过模型对捕捉到的功耗曲线分别按照相应位为 0 或 1 进行分类，得到集合 H_0 与 H_1，用 X_{high} 和 X_{low} 分别表示猜测位分别为 1 或 0 时的功耗，然后计算两个集合对应元素的均差，记 $\varepsilon=\overline{X_{high}}-\overline{X_{low}}$。如果猜测的密钥正确，那么会有差值出现；反之，对集合进行分类等同于用一个随机函数对集合进行分类。由数理统计理论可知，当用一个随机函数将集合一分为二后，当这两个集合中的元素趋于无穷大时，两个子集合的平均值之差将趋于 0。

如果功耗曲线的样本空间足够大、采样噪声的影响足够小、模型选择适当，经过上述差分统计方法可以获得带有尖峰的差分功耗曲线，尖峰位置即为猜测的密钥值。

3 DES 差分功耗分析仿真结果

数据加密标准(Data Encryption Standard，简称 DES)在诞生 20 多年以来经受住了大量密码分析人员的攻击，被证明具有出色的抗数学分析攻击能力。尽管它由于密钥长度太短，将逐渐被更新的 AES 算法所取代，但是以它为基础的 3-DES 算法仍然具有很强的生命力。而且作为一种典型的块密码，对它进行旁路攻击测试仍然具有重要的指导性意义。详细的 DES 算法描述可参见文[9]。

在进行差分功耗分析时，电路的实际功耗可以通过硬件设备进行采集(本文第 4 部分有说明)。但是在电路的设计阶段，当电路没有真实实现时，只能通过一定的软件算法来对设备的功耗情况进行模拟，这就需要建立合适的功耗模型。事实上，对电路进行旁路攻击仿真验证的意义甚至大于对实际电路进行攻击，因为可以在设计阶段就消除攻击的可能性，做到未"亡羊"时先"补牢"。

对功耗在不同的层面上进行抽象，得到的功率消耗模型精度也不相同。不管是寄存器级，还是晶体管级的功耗仿真，需要模拟的器件级别都比较低，数量会很庞大，结构也很复杂，整个工作量和数据量都太大而难以实现。因此，我们就简化为从软件(操作数)一级来对芯片的功率消耗进行仿真。

要对 DES 密码算法进行 DPA 攻击仿真实验，其关键问题是 DES 算法运行时功耗情况模拟。对 DES 密码算法运行时产生的功耗通过汉明距离功耗模型[8]来进行仿真。其思想是在 DES 密码程序(高级语言)中，涉及到数据处理(翻转)的位置设置为一个功耗采样点。这样一共可设置 83 个功耗采样点，其分布情况见图 2。当然，在实际运行时，高级语言需要编译成机器代码，这样产生功耗的语句将会大大增加，功耗采样点也应该相应增加。但是，我们的仿真实验表明，即使是在高级语言级的功耗仿真，DPA 的结果也是有效的。

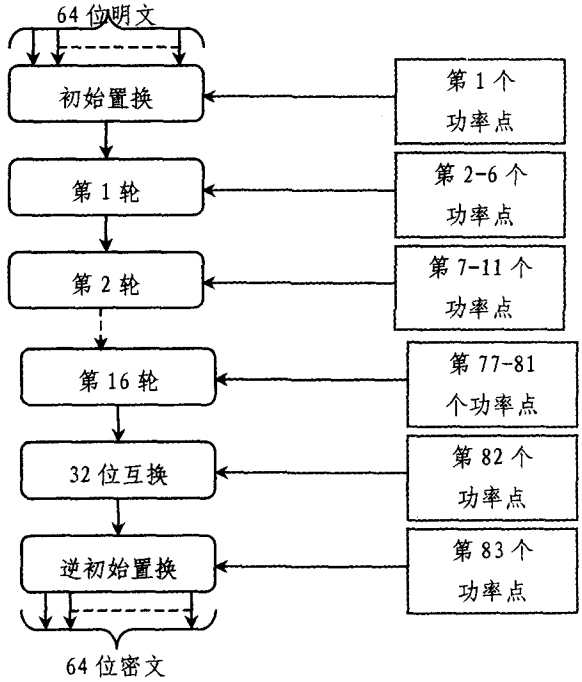

图 2 整个 DES 加密算法中的 83 个模拟功率点，其中每一轮加密有 5 个

仿真实验所用的配置情况为：硬件：2.53GHz 奔 4 处理器，512M 内存；软件：Windows XP＋SP2 操作系统，VC＋＋6.0。

开发的 DPA 仿真工具 DPA_Show 可以完成 DES 加解密、DPA 仿真攻击，以及最后的穷举搜索。试验显示，在明文样本量为 2000 的时候，DPA 仿真攻击的成功率几乎达到 100%。整个攻击耗时不超过 3min。如果不考虑攻击效果的图形化输出，攻击的核心程序耗时不超过 1min。仿真攻击结果在文[10]中已给出。

4 单片机 DES 加密实现差分功耗分析实验

仿真实验验证了 DPA 技术的有效性，因此作者考虑进一步将它应用到具体硬件实现电路中，验证其在真实硬件环境下的有效性。实验配置以及设计实验的电路原理图见图 3。

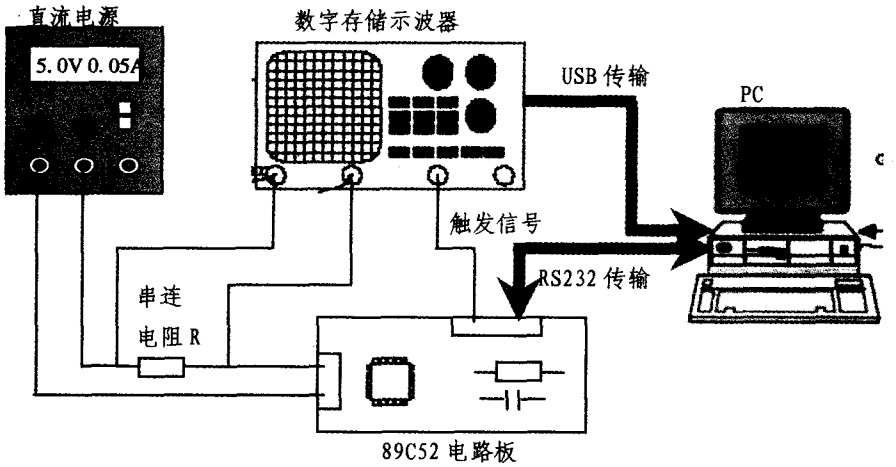

图 3 DPA 实验电路原理图

在目标电路板上由 AT89C52 单片机运行 DES 加密程序，其中密钥预先存储在单片机中。在目标电路板和稳压电源之间串连一个电阻 R，并由数字存储示波器通过测量电阻 R 上的压降的变化来观测单片机电路板的功耗变化。在 PC 机上用 LabView 编写了控制数字存储示波器的虚拟示波器，并由该虚拟示波器来控制数字存储示波器实时向 PC 机传输功耗波形数据，实现了数据采集的完全自动化。

在 10^6 个明文样本的条件下得到了理想的结果。图 4 给出了猜测 DES 第 16 轮子密钥中的 6 位密钥时获得的 64 条差分功耗曲线中的 3 条。其中第一条差分曲线对应的是猜测正确的密钥，后两条对应的是猜测错误的密钥。可以看到，只有在正确密钥对应的差分功耗曲线上才出现了明显的尖峰。通过实验，我们获取了 DES 第 16 轮完整的 48 位密钥。剩余的 8 位密钥同样可以运用穷举方法获取。实验情况完全验证了仿真程序的结果。

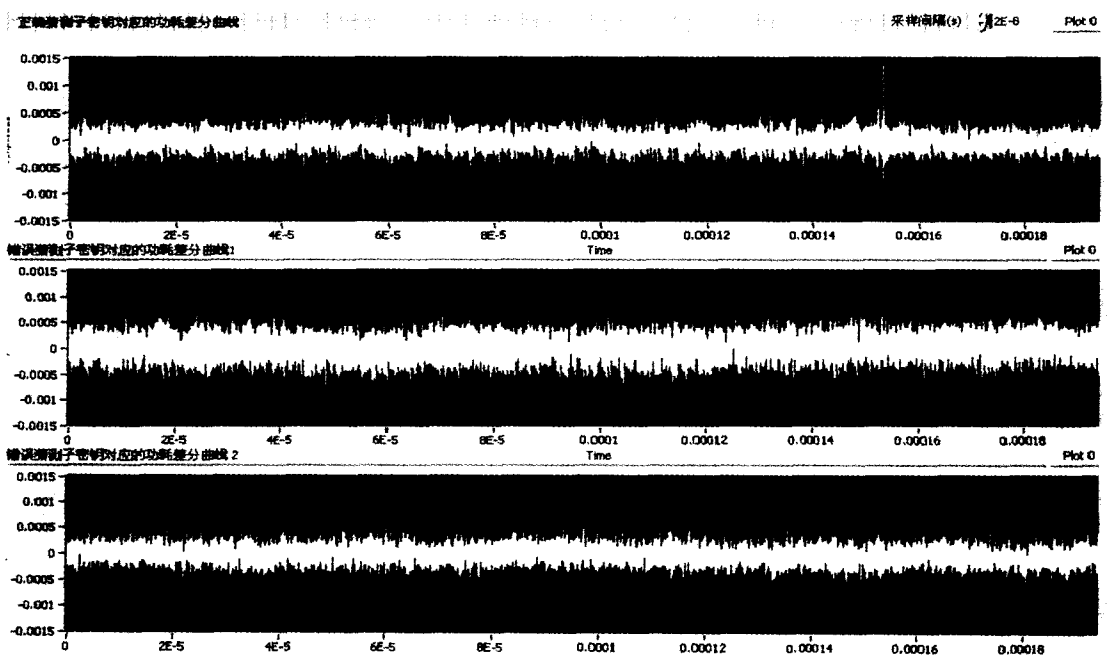

图 4 猜测密钥对应的差分功耗曲线，其中第 1 条对应正确的密钥猜测

结论及今后的研究方向 在分析了 DPA 的原理和方法的基础上，完成了对 DES 加密算法的 DPA 攻击的仿真实现。在 10^3 个明文样本条件下，成功获得了 DES 第 16 轮加密的 48 位密钥。之后对运行在 AT89C52 单片机上的 DES 加密

程序进行实际的 DPA 攻击实验，在 10^6 个明文样本的条件下，成功获得了 DES 第 16 轮加密的 48 位密钥。在验证仿真方法正确性的同时进一步证明了 DES 加密实现面对 DPA 攻击的脆弱性。

下一步工作包括两个方面：一是改进 DES 加密算法，使其能够防护 DPA 攻击，并通过仿真和实验平台对防护方法进行验证；二是对高级加密标准(advanced encryption standard, AES)实现进行 DPA 仿真和实验攻击，研究其面对 DPA 攻击的脆弱性，并提出防护措施。

参 考 文 献

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

2 Messerges T S, Dabbish E A, Sloan R H. Examining SmartCard Security under the Threat of Power Analysis Attacks. IEEE Transactions on Computers, 2002,5: 541～552

3 den Boer B, Lemke K, Wicke G. A DPA attack against the modular reduction within a CRT implementation of RSA. In: Kaliski B S, Koç Ç K, Paar C, eds. Cryptographic Hardware and Embedded Systems - CHES 2002, Lectures Notes in Computer Science (LNCS)[C], Springer-Verlag, 2002

4 Akkar M L, Bevan R, Dischamp P, et al. Power analysis, what is now possible. In: Okamoto T, ed. Lectures Notes in Computer Science (LNCS), Springer-Verlag, 2000

5 Joye M, Paillier P, Schoenmakers B. On Second-order Differential Power Analysis. In: Rao B S J R, ed. Cryptographic Hardware and Embedded Systems - CHES 2005 [C], Edinburgh, UK: Springer-Verlag, 2005. 293～308

6 Chari S, Rao J R, Rohatgi P. Template attacks. In: Kaliski B S, Koç Ç K, Paar C. eds. Cryptographic Hardware and Embedded Systems - CHES 2002, Lectures Notes in Computer Science (LNCS)[C], Springer-Verlag, 2002

7 NSA tempest series. http://cryptome.org/#NSA——TS

8 Canovas C, Clédière J. What do S-boxes Say in Differential Side Channel Attacks? http://cecile.canovas@cea.fr. 2004

9 Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3): Data Encryption Standard

10 陈开颜，赵强，张鹏，等. DES加密实现的差分功耗分析仿真. 军械工程学院学报，2006,3:41～43

(上接第 28 页)

界 Petri 网最小化化简的算法，为有界 Petri 网自动化化简提供了方法。

参 考 文 献

1 Peterson J L. Petri 网理论与系统模拟(吴哲辉译)[M]. 徐州：中国矿业大学出版社，1989

2 王培良，蒋昌俊. Petri 网的并操作[J]. 西北大学学报，1997,27(s):111～114

3 Jiang Changjun, Wu Zhehui. Net Operations [J]. Joural of Comput. Sci. &Technol, 1992,7(4):333～344

4 蒋昌俊. Petri 网的行为理论及其应用[M]. 北京：高等教育出版社，2003

5 吴哲辉. Petri 网导论[M]. 机械工业出版社，2006

6 许安国，吴哲辉. 加权 T-图的保性变换[J]. 计算机学报，1997,20(11):1038～1043

7 许安国，蒋昌俊. 带标识的加权 T-图化简[J]. 电子科学学刊，1998,20(5):655～662

8 蒋昌俊. 加权 T-图的几种化简运算[J]. 通讯学报，1994,15(2):97～102

9 Murata T. Petri nets: Properties Analysis and Applications [J]. Proc. Of The IEEE, 1989,77(4)

10 吴哲辉，蒋昌俊. 有界 Petri 网的可达图到网图的转换算法[J]. 软件学报，1992,3(1):23～29

11 Hopcroft J E, Ullman J D. Introduction to Automata Theory, Languages and Computation [M]. Addison-Wesleg, 1979

12 吴哲辉. Pumping 引理的 petri 网描述--Petri 网语言属型的一组判定条件[J]. 计算机学报，1994, 17(11):853～858

13 陈火旺，等著. 程序设计语言编译原理(第三版)[M]. 国防工业出版社，2000

14 张立昂，等译. 计算理论导引[M]. 机械工业出版社，2000

15 张继军，吴哲辉. 下推自动机的状态转换图与下推自动机的化简[J]. 计算机科学，2006,33(3):271～274

16 张继军，吴哲辉. Petri 网的分层递归模型[J]. 系统仿真学报，2003,15(s):89～92

17 蒋昌俊. 离散事件动态系统的 PN 机理论[M]. 北京：科学出版社，2000

18 袁崇义. Petri 网原理与应用[M]. 电子工业出版社，2005

(上接第 55 页)

33 Zerkle D, Levitt K. NetKuang - A Multi-Host Configuration Vulnerability Checker. In: Proceedings: 6th USENIX Security Symposium, San Jose, California, The USENIX Association, 1996. 195～201

34 Staniford-Chen S, Cheung S, Crawford R, et al. GrIDS - A Graph-based Intrusion Detection System for Large Networks. In: Proceedings: 19th National Information Systems Security Conference, Baltimore, Maryland, National Institute of Standards and Technology and National Computer Security Center, 1996. 361～370

35 Ou Xinming, Boyer W F, McQueen M A. A Scalable Approach to Attack Graph Generation. In: Proceedings of the 13th ACM conference on Computer and Communications Security, 2006. 336～345

36 Li W. An Approach to Graph-based Modeling of Network Exploitations: [Ph D Dissertation]. Department of Computer Science and Engineering, Mississippi State University, Mississippi State, Mississippi, 2005

37 林崇颐. 适应于多量弱点资讯之智慧型攻击图形产生器:[学位论文]. 中原大学，2003

38 Helmer G, Wong J, Slagell M, et al. Software Fault Tree and Colored Petri Net-based Specification, Design and Implementation of Agent-based Intrusion Detection System. Requirements Engineering, 2000,7(4):207～220

39 McDermott J. Attack Net Penetration Testing. In: Proceedings: 2000 New Security Paradigms Workshop (NSPW'00), Cork, Ireland, ACM/SIGSAC, 2000. 15～21

40 Steffan J, Schumacher M. Collaborative Attack Modeling. In: Proceedings: 2002 ACM Symposium on Applied Computing (SAC 2002), Madrid, Spain, ACM/SIGAPP, 2000. 253～259

41 Ou X, Govindavajhala S, Appel A W. MulVAL: A logic-based network security analyzer. In: 14th USENIX Security Symposium, Baltimore, MD, USA, August 2005

42 Noel S, Jajodia S. Managing attack graph complexity through visual hierarchical aggregation. In: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, 2004. 109～118