高级DPA理论与实践

——迈向安全嵌入式电路的安全极限

Advanced DPA Theory and Practice

Towards the Security Limits of Secure Embedded Circuits

【美】艾瑞克·佩特斯（Eric Peeters） 著
王竹 黄伟庆 孙德刚 周新平 欧长海 张仁军 译

国防工业出版社
National Defense Industry Press
Springer

装备科技译著出版基金

高级 DPA 理论与实践

——迈向安全嵌入式电路的安全极限

Advanced DPA Theory and Practice

Towards the Security Limits of Secure Embedded Circuits

(美)艾瑞克·佩特斯(Eric Peeters)著

王 竹 黄伟庆 孙德刚

周新平 欧长海 张仁军 译

国防工业出版社

·北京·

著作权合同登记　图字:军-2015-080 号

图书在版编目(CIP)数据

高级 DPA 理论与实践:迈向安全嵌入式电路的安全极限/(美)佩特斯(Peeters,E.)著;王竹等译. —北京:国防工业出版社,2016.3

书名原文: Advanced DPA Theory and Practice——Towards the Security Limits of Secure Embedded Circuits

ISBN 978-7-118-10472-1

Ⅰ.①高… Ⅱ.①佩… ②王… Ⅲ.①微处理器—系统设计 Ⅳ.①TP332

中国版本图书馆 CIP 数据核字(2016)第 034237 号

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号　邮政编码 100048)
北京嘉恒彩色印刷有限责任公司
新华书店经售

*

开本 880×1230　1/32　插页 6　印张 5¼　字数 138 千字
2016 年 3 月第 1 版第 1 次印刷　印数 1—2000 册　定价 45.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

目录

第三部分 统计工具与高阶攻击

第四部分 迈向理论指导下的侧信道分析

第一章

引 言

故事发生在一家比利时大使馆的二楼，爱丽丝正在给她的同事鲍勃写秘密邮件。她不知道，在街对面的一座相邻的大楼里，他们的老对手伊夫，正在将天线对准二楼办公室的窗口。更令她想不到的是，她屏幕上的东西正在被记录处理，并且显示在伊夫的屏幕上。爱丽丝对大使馆的隐私保护以及自己设置的安全协议有足够自信，认为这足以保证一个安全的环境。但她错了，因为伊夫发现了一条“侧信道”。

最早的这种攻击技术被称为 TEMPEST。

微芯片、显示器、打印机以及所有的电子设备可以通过空气或导体（例如电线或水管）辐射信号[tem]，为此，美国政府制定了以 TEMPEST 为代号的一组标准，用于限制电子设备中电或磁的辐射发散。

TEMPEST 标准的目的是为了防止设备在处理、传输或存储敏感信息的过程中出现无意的泄漏。

目前，现实生活中有各种各样的微电子设备，它们融入到生活的方方面面，使生活变得方便。其中一些微电子设备嵌入了完整的计算机，包括存储器、模拟块、算术逻辑单元（ALU），以保障以下设备的安全：ATM、SIM 卡（手机），ID 卡，社会担保卡，身份确认，签名等。直到 20 世纪 90 年代中期，智能卡仍被当作黑盒。相关应用的机密性，完全取决于智能卡内部实现的密码算法。密码系统经常被证明足够安全，并且在大多数系统，安全性仅仅依赖于算法本身（即密钥与消息的混合方式）。事实则不然，设备在运行过程中存在着敞开的后门使得攻击者可以加以利用并恢复出其中的敏感信息。本书的研究集中在其中两

种重要攻击方式:设备的能量消耗和电磁发射。

虽然在其他敏感领域的应用中,TEMPEST 问题早被知晓(例如,早在 1951 年,美国驻莫斯科大使馆发现大量密封窃听器),但对嵌入式设备的侧信道技术直到 1996 年的计时攻击的出现才被第一次公开提出。计时攻击的概念第一次出现在 Paul Kocher 的文献[Koc96]中。文中指出,安全算法执行过程中的时间波动可能同密钥相关,记录下这些时间波动,运用适当的统计方法就有可能找出正确密钥。两年后,Paul Kocher 根据设备的能量消耗,提出了另一种侧信道攻击,这是侧信道攻击研究的真正开始,在这一年同时创办了 CHES① 会议(CHES 会议旨在收集研究人员在此特定领域的贡献)。

各种各样的泄漏信号都有可能成为攻击者可以利用的信息,从而对设备进行侧信道攻击,因为这些信号携带着与设备行为相关的信息。被研究最多的是计时攻击和能量消耗攻击,因为这两种攻击方法的实验装置简单(例如,能量分析最主要的技术,只需在电源线上串联一块小电阻)。此外,电磁辐射和红外线辐射也被研究,但相对较少。

侧信道攻击对智能卡的设计者和 IC 安全而言,具有挑战性。一方面,智能卡市场对成本高度敏感,当涉及数百万个芯片时,每个芯片几美分的差异都会造成很大的影响。另一方面,侧信道攻击是一个严重威胁,即使它们的初始成本可能较高(一个有足够大的带宽和足够精确的示波器大约 10000 欧元),而它们的平均成本却十分低廉(据 Cryptography Research Inc. ② 的 Joshua Jaffe 透露,每个芯片不到 1 美元)。因此,任何防护措施都必须面对非常严格的成本—效益检测,这种检测在其他 IT 产品中是不常见的。换句话说,设计者必须在不同的成本和卡内机密信息的价值之间找到良好的平衡。

为了读者更好的理解,本书将侧信道攻击按两种方法分为四类:其中一种分类方法将攻击分为入侵式攻击和非入侵式攻击;另一种则分为主动攻击和被动攻击。第一类攻击按照攻击者是否侵入到集成电路

---

① 密码硬件和嵌入式系统研讨会:http://islab.oregonstate.edu。

② 信息来源:Cryptography Research Inc 在 2006 年 6 月是 Ecrypt UCL 暑期学校的报告。

的内部以获取有用信息(例如逆向工程),或者直接探测设备内部的部件(例如微探测)来区分,侵入到电路的称为入侵式攻击,否则称为非入侵式攻击。第二类攻击按攻击者的攻击手段区分,主动攻击通常诱导密码设备的运行环境发生改变,并观察设备的反应(通过电源或时钟变化中断处理器,强磁场或强电场,激光器,重离子束……)。与主动攻击相反,被动攻击只是检测密码设备的一条或多条信道(即泄漏源),并使用记录的泄漏信息恢复出存储在内部的秘密信息(即密钥,代码,……)。在这种攻击方式下,攻击者的行为并不影响设备正常的运行环境。因此与主动攻击相比,检测被动攻击要困难的多。

本书的目标有两个方面:一方面,希望从泄漏的角度(源)探讨能量和电磁侧信道泄漏的可能性,并建立相应的实际模型。即关注下列问题:

· 如何测量能量和电磁是可行的?实验装置应该如何设计?

· 侧信道信号的来源是什么?一个安全设备的哪些部件泄漏最严重(ALU,存储器,时钟信号等)?

· 能否建立统一的能量消耗模型和电磁发射模型?

· 如何才能提高测量技术?

· 哪些信号处理技术可以使用?

· 哪些统计工具可用于分析一次测量中包含的信息?

另一方面,针对已经建立了的模型,本书希望研究侧信道攻击的理论极限。也就是说,充分理解侧信道攻击所构成的威胁,这将是第二部分探讨的核心问题,此问题可以描述如下:

对于一个实现,是否可能存在针对侧信道安全的理论评估?

为了回答这个问题,本书试图给设计者提供一个完整框架,使得他能够对系统实现的安全性进行评估。为了达到这个目的,本书引入了基于信息论的侧信道泄漏模型。在完整的背景知识建立之后,对于不同的防范措施,如噪声产生器、布尔掩码,利用该框架进行安全评估。并在此基础上,尝试给出防物理泄漏设计和实现的定义。

从实用和理论的角度将本书的结构分为四个主要部分:

第一部分对侧信道攻击作了一个简明的综述,分析了不同类型的

攻击，并特别关注成熟的能量分析和近场电磁分析。在这部分的最后，对常用的防御措施进行了介绍。这些防御措施在不同层面抵抗侧信道攻击：逻辑层（使用比 CMOS 更平衡的逻辑结构），硬件层（即噪声产生器），软件层（即布尔掩码）。

第二部分包括三章。其中，第一章尝试根据能量消耗和电磁辐射建立泄漏模型，其他两章侧重于实验装置的实现，需要的实验设备，提高测量质量所需要的后处理方法，以及详细说明 CMOS 设备中能量消耗和电磁泄漏的起源。

在第三部分，本书介绍可以恢复出隐藏在测量数据中秘密信息的多种统计方法。根据所需恢复信息的多少将这些统计方法分为三类，即：需要很少关于泄漏源的信息的方法（即非刻画方法）；需要部分泄漏源和泄漏模型信息的方法，如需要一些统计信息（即设备刻画方法）和最后一类方法需要泄漏源的全部信息（即密钥刻画方法：模板攻击）。此外，应用无监督方法研究了高阶布尔掩码的抵抗能力，得出的结果是抵抗能力依赖于侧信道泄漏统计分布特征。

在最后一部分，将介绍一个理论框架，该框架旨在让设计者也可以对自己的实现方案的安全性进行可操作的评估。这个框架建立在两个评估标准上，一个是成功率，它是不同攻击类型攻击效果做比较时的唯一标准。另一个是互信息，信息论的一个概念，即通过一次（或一些）观测揭示出的信息的多少来评估方案设计的优劣。在后面的章节里，本书会论述只有将这两个标准相结合，才能得出对不同实现的物理安全性简单易行的评估方法。

1.1 嵌入式安全设备

智能卡的概念出现在 20 世纪 70 年代。在那个阶段，众多的研究机构对于这个包括电路元件和存储器的塑料卡片都有各自构想。由此，也孕育出了来自世界各地的发明人，如 Ellingboe，Halpern，Gretag 等，提出了多项有关智能卡的专利申请。

第一张真正意义上的智能卡诞生于 1974 年，身为记者和

Innovatron 公司负责人的法国人 Roland Moreno，第一次成功地将集成电路技术应用于一个电子储值的戒指应用项目上。这是存储式卡的第一次出现。同年 9 月，第一个塑料卡片被制造出来（图 1.1），它是智能卡的前身，已经诞生了超过四分之一个世纪时间。

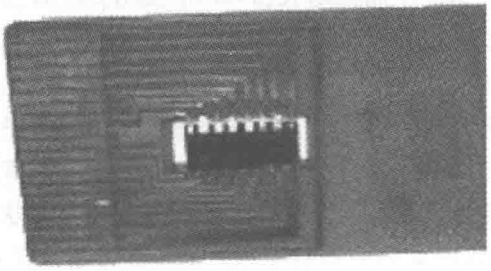

图 1.1　第一个卡片

1979 年，Bull CP8 公司成立，在它的技术领导层，Michel Ugon 对这种新出现的存储式卡产生了强烈的兴趣。于是，第一个嵌入微处理器的卡①在 1979 年诞生了，它包含一个存储块和一个 Motorola 微处理器。同年，Schlumberger 加入 Innovatron 公司的核心层，智能卡的研究开始在 Schlumberger 的“存储卡和系统部”进行。

一年后的 1980 年，法国银行的一家财团使用智能卡技术发明了一种新的支付方式，这意味着智能卡将变成未来的银行卡。在此基础上，Bull 公司，Schlumberger 公司和 Philips 公司深化了智能卡的概念，并在 1984 年开始将第一批银行储值卡商业化。1985 年，Bull 公司交付了首批装有微处理器的卡。

同时，对于智能卡可能应用领域的研究也在慢慢地扩展，智能卡在健康体系和社会保障体系起到重要的作用：使用智能卡可以给每个病人建立一张记录健康情况健康卡，它能更详细地记录持卡人的健康状况。通信业也表现出了对智能卡发生了极大的兴趣。1983 年法国电信的大众通信集团（the General Direction of France Telecommunication，

① 这项专利在 1978 年 4 月 25 日被申请。

法国电信的前身)推出了自己的电信卡,允许提取客户手机账单的每一条通信。但在1984年出现了著名的公共电话卡,由Schlumberger公司为法国电信发明。公共电话卡提供了微模块,这类卡正经历智能卡历史上最辉煌的成功:公用电话逐渐被智能电话取代。新的公用电话与预付款的电话卡同步高速增长:1986年卖出200万张卡,而1991年每月卖出的卡就超过600万。这一成功很快超越了法国甚至欧洲的极限,并达到全球层次。从此,智能卡成了社会的新媒介。

今天,凡需要便捷、合理的安全密码令牌的地方,都有智能卡的应用:电子钱包,个人健康信息存储,付费电视,SIM手机卡等。零部件设计和制造的高速发展推动了智能卡产业的增长。微模块智能卡的尺寸与信用卡相同,常由柔韧的塑料制成(聚氯乙烯或PVC),并且卡中嵌入了一个微模块,微模块中包含一个带存储器和微处理器的单硅集成电路芯片。每个微模块的表面都有按国际标准设计8个金属垫:VCC(电源电压),RST(对智能卡的微处理器进行复位),CLK(时钟信号),GND(接地端),VPP(编程电压或写入电压),I/O(串行输入/输出线)。剩余两个金属垫为将来的应用保留(RFU)。只有I/O和GND接口必须符合国际标准,其他接口的标准都是可选的。

当智能卡插入卡片接入设备(CAD)(例如销售终端)后,金属垫通过金属引脚与CAD接触,使得智能卡与CAD得以通信。当接入CAD后,智能卡总是处于复位状态,这一行为导致智能卡通过发送一个回答—复位消息进行响应,以通知CAD有哪些规则控制与智能卡的通信以及进行事务处理。

为了能够执行指令以支撑智能卡的功能,智能卡板上的微模块由以下关键部件组成:

- 微处理器单元(MPU)执行编程指令。通常,老版本的智能卡基于相对较慢的、8位嵌入式微控制器。20世纪90年代的趋势已经转向使用定制的控制器,使用32位的精简指令集(RISC)处理器,处理器的主频范围为25~32MHz。
- I/O控制器管理卡片接入设备(CAD)和微处理器之间的数据流。

• 只读存储器(ROM)或程序存储器。芯片制造商将指令永久地刻录到内存中。这些指令(如什么时候电源应该激活,管理口令的程序)是芯片操作系统的基础。

• 随机存取存储器(RAM)或工作存储器,用于暂时存储计算结果或输入/输出的交互结果。RAM 是不稳定的存储器,断电后信息立即丢失。

应用存储器,最常见的是 EEPROM(带电可擦除可编程只读存储器),能够用电擦除和重写。根据国际标准,应用存储器应在没有电源的情况下可以将数据保存 10 年,并且在卡的生命周期内至少支持 10000 次的读写行为。通过执行应用程序,应用存储器将信息存储在卡上。最后,在多种卡和多个终端厂商的应用环境中,有一些标准保证了互用性和兼容性。早在 20 世纪 80 年代,IC 卡的标准化就已经在国家层面和国际层面进行。智能卡基本的世界范围标准由国际标准化组织制定,这一组织代表了 70 多个国家,目前标准化工作仍在进行中。ISO7816 系列标准是 IC 卡的国际标准。

1.2 本书涉及的研究对象

本书的研究主要集中在安全应用领域的两类部件:微控制器和 FPGA。选择微控制器,因为它的结构(ALU、闪存、总线等)在许多方面同智能卡相似。选择 FPGA 则跟随当前的使用趋势,即使用可重构的硬件设备(现场可编程门阵列,FPGA)以缩短一些安全应用进入市场的时间(例如,intoPIX 公司开发的安全媒体模块)。

这里简要列出这些部件的主要特征,读者若想获得进一步的信息可参考相应的手册。

• Microchip 公司的 PIC16F877 微控制器:它是一个 8 位的 RISC 微控制器,嵌入到 0.9um 的微芯片内部。该微控制器基于 Harvard 体系结构,将指令以及数据的存储路径和信号路径分开。PIC16F877 有一个快速程序存储器(闪存),并且它的结构基于一个中央工作寄存器。

• Atmel 公司的 ATMEGA88r：也是一个 8 位微处理器，由 Atmel 公司使用 0.35μm 技术制造。ATMEGA88r 在许多方面同 PIC 相似，不同之处在于，ATMEGA88r 的操作池要大得多，而且有许多工作寄存器（通用寄存器）。

• Xilinx 公司的 Spartan Ⅱ FPGA：在初级实验中，首先使用了普通的 Virtexr Ⅱ 开发板，随后在一个带有 PQ208 软件包的专用开发板 Spartan Ⅱ XC2S200 FPGA 上进行了所有的实验。Spartan Ⅱ FPGA 由 Xilinx 使用 0.12μm 的技术制造。

参 考 文 献

[Bar71] Barjavel, R. (1971). La Nuit des Temps.

[KJJ99] Kocher, P. C., Jaffe, J., & Jun, B. (1999). Differential power analysis. In M. J. Wiener(Ed.), CRYPTO, LectureNotes in Computer Science (Vol. 1666, pp. 388-397). Heidelberg:Springer.

[Koc96] Paul C. K. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz (Ed.), CRYPTO, Lecture Notes in Computer Science (Vol. 1109, pp. 104-113). Verlag: Springer.

[tem] The Complete, Unofficial TEMPEST Information Page.

[Ugo86] Ugon, M. (1986). L'odisse de la carte puce.

第一部分

安全嵌入设备和侧信道攻击