数学名著译丛

能量分析攻击

〔奥〕 Stefan Mangard　Elisabeth Oswald　Thomas Popp 著

冯登国　周永彬　刘继业 等 译

科学出版社
www.sciencep.com

数学名著译丛

能量分析攻击

〔奥〕Stefan Mangard　Elisabeth Oswald　Thomas Popp　著
冯登国　周永彬　刘继业　等　　译

科学出版社
北京

图字：01-2008-5507 号

内 容 简 介

能量分析攻击旨在通过分析密码设备的能量消耗这一物理特性来恢复设备内部的秘密信息. 这种基于实现特性的密码分析对广泛应用的各类密码模块的实际安全性造成了严重威胁. 本书是关于能量分析攻击的综合性专著, 系统阐述了能量分析攻击的基本原理、技术方法以及防御对策的设计与分析.

本书可以作为密码学、电子工程、信息安全等专业的教材, 也可以供相关专业人员参考.

图书在版编目(CIP)数据

能量分析攻击 /〔奥〕Stefan Mangard 等著; 冯登国等译. —北京: 科学出版社, 2010

(数学名著译丛)

ISBN 978-7-03-028135-7

Ⅰ. 能… Ⅱ. ① 曼… ② 冯… Ⅲ. ① 信息系统-安全技术 ② 密码-理论 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字(2010) 第 121301 号

责任编辑: 赵彦超 张 扬 / 责任校对: 宣 慧
责任印制: 钱玉芬 / 封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

双源印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 8 月第 一 版 开本: B5(720×1000)
2010 年 8 月第一次印刷 印张: 18 3/4
印数: 1—2500 字数: 250 000

定价: 58.00 元

(如有印装质量问题, 我社负责调换)

译 者 序

1996 年, Paul Kocher 博士 (2009 年 1 月当选为美国工程院院士) 首次提出计时攻击的重要奠基性思想并发表相关研究成果. 此后十余年来, 侧信道攻击及防御对策研究便成为密码学研究中的一个重要分支, 受到了国际学术界与产业界的广泛关注. 能量分析攻击是最重要、最有效的侧信道攻击形式之一, 对诸如智能卡这样的智能设备的实际安全性造成了极大的威胁, 相关研究是当前侧信道攻击研究领域的热点方向. 近年来, 内嵌密码模块的智能设备和嵌入式设备已广泛应用于各类信息产品与通信系统中, 在这类应用环境与应用模式下, 能量分析攻击对系统安全性造成的实际威胁将更加严重.

能量分析攻击是什么? 实施能量分析攻击需要什么样的设备与技术条件? 这种攻击对密码设备的实际安全性将会造成什么样的影响? 如何设计可靠、高效、低廉的防御对策来有效地防御这类攻击? 如何客观、合理地评估各种防御措施的有效性? 本书作者在侧信道攻击、防御措施设计以及有效性评估方面进行了一系列先锋性的研究和实践, 本书就是他们近几年来一系列优秀工作成果和经验的总结, 将会对上述问题进行解答.

正所谓 "知己知彼, 百战不殆", 试图有效地抵御能量分析攻击, 最有效的途径就是深入地剖析它. 本书系统地论述了能量分析攻击的理论基础、技术条件、实施方法以及相应的防御对策; 基于一系列的实验结果和理论分析, 将能量分析攻击的相关研究成果融入一个具有创新性的理论框架. 同时, 本书也是国际上关于能量分析攻击 (甚至是侧信道攻击) 研究的第一部学术专著. 因此, 在承担国家自然科学基金、国家高技术研究发展计划以及北京市自然科学基金等相关项目的过程中, 我们组织项目组主要成员翻译了本书, 希望对国内密码学的研究与密码技术的应用起到一定的推动作用.

参加本书翻译的主要成员有冯登国、周永彬、刘继业、陈海宁、黄金刚、范丽敏、于振梅等, 冯登国对全书进行了统稿与校对.

本书的翻译工作得到了国家自然科学基金 (编号: 60833008 & 60503014)、国家高技术研究发展计划 (编号: 2008AA01Z417) 以及北京市自然科学基金 (编号: 4072026) 的资助, 特此致谢.

译 者

2009 年 11 月于北京

序

我们不了解电, 但这并不妨碍我们使用它

——Maya Angelou

研究密码设备的防篡改特性之初, 我无力购买实施物理攻击所需要的昂贵芯片逆向工程设备, 这便提出了一个重大问题: 公司客户需要有关分析结果, 但是我们却无法使用那些当时即属众所周知的攻击技术.

我从如下简单问题开始入手: 对攻击者而言, 存在哪些可用却未包含于密码协议假设中的信息? 之前, 我已经发现微妙的计时变化可能会危及密钥. 因此, 我决定弄清楚设备的能量消耗是否也可以揭示出一些有用的信息.

将一台价值 500 美元的模拟示波器 (购自 Fry's Electronics) 搬回家数小时之后, 我和同事 Joshua Jaffe 便首次观察到能量迹. 我们首先对一个执行 RSA 算法的智能卡进行实验, 并发现可以从智能卡的能量迹中识别出主要的算法特征. 不久之后, 我们便掌握了识别平方和乘法操作的方法, 并使用 SPA 攻击第一次成功地获取了密钥. 此外, 我们还分析了 DES 实现, 并发现它们同样可以被破译, 尽管我们只能在夜间进行攻击实验 —— 因为在白天, 实验室的光线太强, 我们无法看清廉价示波器显示屏上的信号.

接下来的几个月中, 我们搭建了数字数据采集系统, 以期实现更复杂的分析. 我们还开发了可视化软件, 并实现了包括 DPA 在内的多种分析技术. 通过对无数产品进行测试, 最终发现我们所分析的所有智能卡以及其他防篡改设备均可以被破译. DPA 攻击的能力不只是令人惊叹, 简直可以用 "非常恐怖" 来形容.

与此同时, 我们也致力于抵抗能量分析攻击的防御对策的设计. 防御对策的设计十分困难, 因为 DPA 攻击采用的统计手段能够辨析出淹没在噪声中的细微相关性. 同时, 消除信息泄漏几乎不可能, 因为电子运动始终消耗电能, 并产生电磁场. 现在, 我们公司已经从这项研究工作中获得了多项专利. 为了不使个人或公司感到惊讶, 有必要指出, 如果您在产品设计中使用了 DPA 防御对策, 请注意这些专利的存在.

有趣的是, SPA 和 DPA 在很长的一段时间内都没有被发现. 原因很简单: 该研究领域不属于任何人的研究范畴. 密码学家关注于实现数学强度, 而工程师则要对硬件和软件负责. 攻击研究也被严格互补地划分为对算法的研究和对物理安全性的研究. 几乎没有密码学家在开发实际的产品, 也很少有工程师了解密码学. 我希

望读者阅读本书时, 会考虑到一些可能被忽视的其他安全问题.

公众了解 DPA 之后的近几年来, 防篡改研究十分活跃. 许多会议都在关注这一话题. 本书作者以及其他研究者已经把 DPA 攻击扩展到了很多新方向, 相关产品也有了很大的改进. 尽管我们公司检验过的大部分产品仍然存在 DPA 脆弱性, 但是如今最好的产品已经具有了优良的抗 DPA 能力. 供应商也已经意识到防篡改是一个异常困难的问题, 所以他们作出的安全性声明也现实得多.

展望未来, 防篡改仍将是一个相当有趣而且很重要的课题. 2007 年, 全球将生产逾 20 亿防篡改芯片, 用于安全通信、支付、打印机耗材、付费电视系统、政府 ID 以及其他不计其数的应用领域. 面向防篡改半导体器件的攻击已经导致了数十亿美元的欺诈和盗版. 密码协议的安全性等同于它所使用的秘密信息的安全性, 这已成为一条准则. 无疑, 关于如何安全地储存和管理密钥, 还有大量未知内容有待探索.

读者将会发现, 本书非常有趣且令人警醒. 卷起袖子准备大干一场吧! 要敢于质疑, 勤于参加学术会议, 并遵纪守法. 最重要的一点, 愿读者从本书中获得乐趣!

Paul Kocher
Cryptography Research Inc. 总裁兼首席科学家
2006 年 9 月于美国旧金山

前　言

能量分析攻击是一种能够从密码设备中获取秘密信息的密码攻击方法. 与其他攻击方法不同, 这种攻击利用的是密码设备的能量消耗特征, 而非密码算法的数学特性. 能量分析攻击是一种非入侵式攻击, 攻击者可以方便地购买实施攻击所需要的设备, 所以这种攻击对智能卡之类的密码设备的安全性造成了严重威胁.

智能卡是应用最为广泛的密码设备. 智能卡公司国际组织 Eurosmart 宣称, 在最近几年中, 具有微处理器的智能卡的市场份额至少翻了一番. 2003 年, 全球范围内发行的智能卡尚不足 10 亿, 而到了 2006 年, 这个数字将超过 20 亿. 在这些智能卡中, 大多数主要应用于电信、金融服务、政府服务、企业安全和付费电视等对安全敏感的行业和部门. 智能卡是这些应用中最关键的部分, 所以其安全性至关重要.

受研发相应防御对策需求的驱动, 科研人员对能量分析攻击进行了深入细致的研究. 能量分析攻击已经成为一个极具吸引力的科研领域. 这一研究需要具有多方面的知识, 包括密码学、统计学、测量技术和微电子学. 能量分析攻击吸引了上述各个科研领域的科研人员, 所以近年来涌现出了大量的相关科研论文. 事实上, 跟踪这些出版物并把握这些文献要旨之间的关系已非常困难. 此外, 目前尚缺乏一本能够使读者熟悉各种不同类型的能量分析攻击及防御对策的介绍性读物. 本书旨在填补这项空白.

本书对能量分析攻击进行了全面的介绍. 首先讨论密码设备、密码设备设计以及密码设备的能量消耗, 接着简要介绍统计学和电子工程, 旨在阐释各种不同的能量分析攻击及防御对策. 本书的预期读者是任何具有密码学、安全或微电子背景的科研与工程技术人员.

本书的结构

本书包括 11 章和两个附录. 前两章是介绍性内容, 其对象是能量分析攻击的初学者和缺乏工程技术背景的读者. 接下来的两章介绍关于密码设备能量消耗的重要内容, 包括能量消耗的测量方法和统计分析方法, 其对象是希望深入了解有关背景信息的读者. 这两章的内容并非理解后续 6 章讨论能量分析攻击及防御对策的必要知识. 然而对于高级主题而言, 这些基础知识是必须的. 最后一章介绍了全书的结论. 下面的列表将对各章节内容进行更具体的介绍.

第 1 章阐释密码学和密码设备之间的关系. 本章对密码设备的各种攻击方式进行综述, 给出能量分析攻击的一个简单示例, 并对能量分析攻击的防御对策进行分类.

第 2 章讨论密码设备的设计与实现. 本章介绍典型半定制化设计流程的工作原理. 此外, 还对逻辑元件, 特别是 CMOS 元件进行一般性介绍.

第 3 章集中讨论基于 CMOS 的密码设备的能量消耗. 本章阐述能量消耗的仿真方法和适用于能量分析攻击的能量消耗模型. 此外, 还将讨论用于能量分析攻击的测量配置.

第 4 章介绍基于统计学的能量迹分类方法. 本章首先讨论能量迹中的单点特征, 并给出量化单点信息泄漏的方法. 接着, 讨论能量迹中多个不同点之间的统计关系. 最后, 简要介绍置信区间和假设检验的原理及其在能量分析攻击中的应用.

第 5 章介绍简单能量分析攻击. 本章表明对能量迹进行直观分析往往可以提供有用的信息. 此外, 还介绍模板攻击和碰撞攻击, 并给出若干用于支撑上述观点的攻击示例.

第 6 章介绍差分能量分析攻击. 本章讨论 DPA 攻击的基本原理, 给出针对 AES 算法软件和硬件实现的 DPA 攻击实例. 所有的这些攻击均基于相关系数. 本章还介绍 DPA 攻击仿真方法与确定攻击所需要的能量迹数量的方法. 此外, 还对异于基于相关系数的其他攻击方法进行综述, 并讨论基于模板的 DPA 攻击.

第 7 章讨论隐藏技术. 本章对诸如乱序操作、随机插入伪操作、均一化能量消耗以及噪声引擎等能量分析攻击的防御对策进行综述. 此外, 还对双栅预充电逻辑结构进行深入探讨.

第 8 章分析隐藏对策的效果. 基于成功实施 DPA 攻击所需要的能量迹数量, 给出评估隐藏对策效果的量化方法. 接着, 讨论基于失调能量迹的 DPA 攻击. 最后, 分析两种双栅预充电逻辑结构的效果.

第 9 章讨论掩码对策. 本章介绍不同类型的掩码对策, 讨论采用软件和硬件方式实现掩码对策时需要特别注意的要点. 此外, 还讨论对逻辑元件进行掩码保护的方法.

第 10 章分析掩码对策的效果. 本章介绍二阶 DPA 攻击破译软件和硬件掩码对策的原理, 对实施二阶 DPA 攻击的几种方法进行比较. 此外, 本章还表明基于模板的 DPA 攻击是一种能够破译掩码对策实现的强大攻击手段.

第 11 章本书的结论.

附录 A 是 Kocher 等发表的关于能量分析攻击的第一篇科研论文 [KJJ99].

附录 B 介绍高级加密标准 (AES), 并简要介绍一种 AES 的软件实现和一种 AES 的硬件实现. 本书中的 DPA 攻击示例均基于这两种实现.

介绍性的第 1 章和背景性的第 2~4 章均在结尾处对各自的内容进行简短总结, 而第 5~10 章则是关于具体的攻击和防御对策, 其结尾处均给出注记和补充阅读材料. 这些注记和补充阅读材料是本书的重要部分, 它们将本书的观点和其他研究联系在一起. 注意, 尽管这些注解和阅读建议是综合性的, 但并非面面俱到. 为

了方便阅读, 我们还给出了术语表和符号说明. 此外, 本书的最后提供了作者索引和主题索引. 本书还提供网站: http://www.dpabook.org. 该网站提供了能量迹以及 Matlab 和 Octave 分析脚本. 网站建设的目的在于便于读者对能量分析攻击及防御对策进行试验.

致谢

如果没有多个机构的资助. 本书的写作不可能完成. 感谢格拉兹理工大学应用信息处理和通信研究所 (IAIK) 的支持. 此外. 感谢奥地利信息安全技术中心 (A-SIT)、奥地利自然基金 (FWF) 以及欧盟委员会 (EC) 对多个能量分析攻击项目的资助.

本书阐述能量分析攻击中所使用的 AES 算法软件和硬件实现由我们的合作者完成. 感谢 Christoph Herbst 在微控制器上实现了多种 AES 算法, 感谢 Norbert Pramstaller 在多种专用硬件上实现了 AES.

我们的很多同事奉献出了大量的宝贵时间, 参与到本书的校对工作中. 特别感谢如下人员的帮助: Martin Feldhofer. Christoph Herbst, Mario Lamberger, Karl Christian Posch, Norbert Pramstaller, Vincent Rijmen, Martin Schläffer 和 Stefan Tillich.

感谢 Vincent Rijmen 和 Joan Daemen 提供 AES 算法的图示, 感谢 Christoph Herbst 为本书所做的封面设计.

此外, 特别感谢三位能量分析攻击的发明者 Paul Kocher, Joshua Jaffe 和 Benjamin Jun 允许我们转载他们的原始 DPA 论文. 此外, 特别感谢 Paul Kocher 为本书作序, 感谢 Joshua Jaffe 给本书以极具价值的评价.

最后, 诚挚地感谢所有在此书编撰过程中为我们提供学术及精神帮助的同事和朋友们.

Stefan Mangard, Elisabeth Oswald, Thomas Popp

2006 年 9 月于奥地利格拉兹

符 号 说 明

变量和函数的意义将在书中初次引用时给予说明. 最重要的全局约定是, 本书采用黑体大写字母表示矩阵, 采用黑体小写字母表示向量. 除非经过转置, 本书中的向量均指列向量. 矩阵中的行、列和元素表示如下: 矩阵 $\boldsymbol{T}$ 的第 j 列表示为 $\boldsymbol{t}_j$, 第 i 行表示为 $\boldsymbol{t}_i'$, 第 j 列的元素 i 表示为 $t_{i,j}$. 下面将给出本书中使用的最重要的变量和函数列表.

ck	$\boldsymbol{k}$ 中正确密钥的索引
ct	DPA 攻击中, 与被攻击中间结果相关的信息泄露在能量迹中的位置索引
$\boldsymbol{C}$	协方差矩阵 (大小为 $N_{\mathrm{IP}} \times N_{\mathrm{IP}}$) 及其估计量
$\mathrm{Cov}(X, Y)$	X 和 Y 的协方差
D	DPA 攻击中使用的能量迹数量
$E(X)$	随机变量 X 的期望
$\boldsymbol{d}$	DPA 攻击中使用的输入值或输出值向量 (大小为 $D \times 1$)
$\boldsymbol{H}$	DPA 攻击中的假设能量消耗值矩阵 (大小为 $D \times K$)
$\mathfrak{h}$	模板
$\mathscr{H}$	模板矩阵
$\boldsymbol{k}$	DPA 攻击中的密钥假设向量 (大小为 $1 \times K$)
k	密钥
k_{ck}	被攻击的密码设备所使用的密钥
K	密钥假设的总数量
μ	正态分布的均值
$\boldsymbol{m}$	均值向量及其估计值 (大小为 $N_{\mathrm{IP}} \times 1$)
m	掩码
m_d	对数据 d 的掩码值
M	掩码可能具有的不同值的数量
n	计算得出的实施 DPA 攻击所需的能量迹数量
N_{IP}	特征点的数量
$p(X = i)$	$X = i$ 的概率
$\Phi(x)$	标准正态分布的累加分布函数
ρ	相关系数
r	相关系数估计量
$\boldsymbol{R}$	DPA 攻击的结果 (大小为 $K \times T$), 通常为一个相关系数估计矩阵
σ	正态分布的标准差

$\boldsymbol{s}$	仿真生成的能量迹
$\boldsymbol{S}$	仿真生成的能量消耗值矩阵
s	标准差估计量
$S(x)$	AES 的 S 盒函数
$\boldsymbol{t}$	能量迹 (大小为 $T \times 1$)
$\tilde{\boldsymbol{t}}$	预处理后的能量迹
$\boldsymbol{T}$	能量消耗值矩阵 (大小为 $D \times T$), 该矩阵的每一行代表一条能量迹
$\tilde{\boldsymbol{T}}$	预处理后的能量消耗值矩阵
$\boldsymbol{T}$	能量迹中点的数量
$\boldsymbol{V}$	DPA 攻击中假设值矩阵 (大小为 $D \times K$)
$\mathrm{Var}(X)$	随机变量 X 的方差
$\bar{x}$	均值估计量

术　　语

3sDL	三态动态逻辑
AES	高级加密标准
ALU	算术逻辑单元
ASIC	专用集成电路
CML	电流模逻辑
CMOS	互补金属氧化物半导体
CRT	中国剩余定理
DES	数据加密标准
DIP	双列直插式封装
DPA	差分能量分析
DPDN	差分下拉网络
DPTR	数据指针
DPUN	差分上拉网络
DR	双栅
DRP	双栅预充电
DSA	数字签名算法
DSDR	双垫双栅
DyCML	动态电流模逻辑
ECC	椭圆曲线密码学
ECDSA	椭圆曲线数字签名算法
EDA	电子设计自动化
EM	电磁场
EMC	电磁兼容性
EMV	Europay/Mastercard/Visa
FFT	快速傅里叶变换
FIPS	联邦信息处理标准
FPGA	现场可编程门阵列
GALS	全局异步局部同步
GF	伽罗瓦域
GPIB	通用接口总线
HD	汉明距离
HDL	硬件描述语言
HF	高频

HMAC	基于杂凑的消息认证码
HSM	硬件安全模块
HW	汉明重量
IC	集成电路
IDEA	国际数据加密算法
IEC	国际电子协会
I/O	输入输出
LCD	液晶显示屏
LSB	最低有效位
LSQ	最小二乘法
MCML	MOS 电流模逻辑
MDPL	掩码型双栅预充电逻辑
ML	极大似然准则
MOS	半导体金属氧化物
MSB	最高有效位
NAND	与非门
NED	正态能量偏移
NIST	(美国) 国家标准技术局
NMOS	n 型半导体金属氧化物
NSA	(美国) 国家安全局
PC	个人计算机; 程序计数器
PCB	印刷电路板
PLCC	带引线的塑料芯片载体
PMOS	p 型半导体金属氧化物
PS/2	个人系统 2
RAM	随机存储器
RC4	Rivest 流密码 4
RC6	Rivest 流密码 6
RFID	射频识别
ROM	只读存储器
RS	推荐标准
RSA	Rivest-Shamir-Adleman
RTL	寄存器传输层
SABL	基于灵敏放大器的逻辑
SFR	专用寄存器
SHA	安全杂凑算法
SNR	信噪比
SPA	简单能量分析

SPICE	增强型集成电路仿真程序
SR	单栅
TEM	横向电磁场
TOE	计算时间
TDPL	三相双栅预充电逻辑
USB	通用串行总线
VHDL	VHSIC 硬件描述语言
VHSIC	超高速集成电路
VML	电压模逻辑
WDDL	波动差分逻辑
ZV	零值

目　　录