<<能量分析攻击>>

图书基本信息

书名：<<能量分析攻击>>

13位ISBN编号：9787030281357

10位ISBN编号：7030281357

出版时间：2010-8

出版时间：科学出版社

作者：Stefan Mangard,Elisabeth Oswald,Thomas Popp

页数：278

前言

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。

<<能量分析攻击>>

内容概要

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。

作者简介

作者：（奥地利）Stefan Mangard （奥地利）Elisabeth Oswald （奥地利）Thomas Popp 译者：冯登国 周永彬 刘继业 等

<<能量分析攻击>>

书籍目录

<<能量分析攻击>>

章节摘录

插图：被动型半入侵式攻击的目标通常是在无需利用或者探测储存单元的数据读取电路的情况下，读取出储存元件中的内容，文献［ssAQ02]公开发表了一种成功的此类攻击。
主动型半入侵式攻击的目标是诱发设备产生故障，这项工作可以通过使用x射线、电磁场或者光学手段等来完成，例如，文献［sA031中发表了关于通过光学手段实施故障诱发攻击的描述。
通常，半入侵式攻击不需要使用实施入侵式攻击所需要的那样昂贵的设备，然而其成本仍然相对高昂，特别地，在现代芯片的表面，选择一个实施半入侵式攻击的正确部位就需要花费一些时间，同时也需要一定的专业知识，关于半入侵式攻击最全面的已公开文献可参见Skorobogatov的博士论文（Sko05），非入侵式攻击非入侵式攻击中，被攻击的密码设备本质上和其正常工作时的状态没有任何区别，也就是说，这种攻击仅仅利用了设备上可被直接访问的接口，设备自身永远不会发生改变，因而实施这种攻击之后不会遗留下任何痕迹，大多数非入侵式攻击都可以借助于价格相对低廉的设备来实施，因此，这类攻击对密码设备的安全性造成了严重的实际威胁，特别地，近几年来，被动型非入侵式攻击受到了极大的关注，这种攻击通常也称为“侧信道攻击”（side-channelattacks，SCA），其中，最重要的侧信道攻击有三类：计时攻击（Koc96）、能量分析攻击（KJJ99）以及电磁攻击（GM001，Qs01）。
除了侧信道攻击之外，还存在主动型非入侵式攻击，这类攻击的目标是在无需拆解设备的情况下诱发设备产生故障，例如，可以通过时钟突变、电压突变或者改变环境温度等手段来诱发密码设备产生故障，关于这类攻击的综述，可查阅文献（BEcN+04）。

<<能量分析攻击>>

编辑推荐

《能量分析攻击》是数学名著译丛。

<<能量分析攻击>>

版权说明