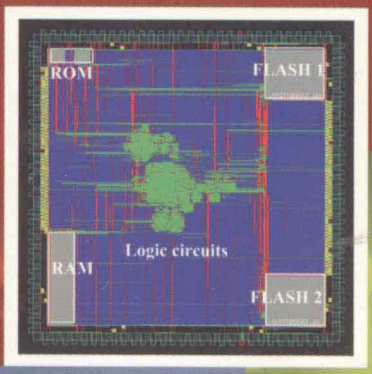
密码安全芯片与侧信道技术

李慧云　李大为　罗　鹏　尹旭程　编著



科学出版社

密码安全芯片与侧信道技术

李慧云　李大为
罗　鹏　尹旭程　编著

科学出版社
北京

内 容 简 介

本书着重探讨密码安全芯片受到的侧信道攻击以及相应的安全措施与安全评估方法。第1章为信息安全简介；第2章介绍通用密码算法，包括对称算法(DES、AES)和公开密钥算法(RSA、ECC)，这些算法实现是侧信道分析攻击的对象；第3章介绍侧信道分析的分类与半导体物理基础；第4章介绍时序攻击；第5章介绍功耗攻击；第6章介绍电磁攻击；第7章讲述侧信道技术与其他密码分析技术的结合应用；第8章讨论侧信道技术的研究热点及未来发展趋势。

本书可供密码安全芯片领域的工程技术人员与科学研究人员参考，信息安全领域的研究生可将本书作为补充读物。

图书在版编目(CIP)数据

密码安全芯片与侧信道技术/李慧云等编著. —北京：科学出版社，2014.1

ISBN 978-7-03-039325-8

I. ①密… II. ①李… III. ①芯片–信息安全–加密技术 IV. ①TN43 ②TP309.7

中国版本图书馆 CIP 数据核字(2013)第 300753 号

责任编辑：余 丁/责任校对：李 影
责任印制：张 倩/封面设计：蓝 正

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
源海印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2014 年 1 月第 一 版 开本：B5 (720 × 1000)
2014 年 1 月第一次印刷 印张：7 1/4
字数：132 000
定价：45.00 元
(如有印装质量问题，我社负责调换)

前　言

1998年Paul Kocher等学者提出侧信道分析攻击技术，翻开了密码分析技术新篇章。当时主要以便携式密码设备，如智能卡(IC卡)等为主要侧信道攻击对象。因为智能卡是当时身份认证和金融支付类的新兴电子载体。

经过网络信息技术10余年的迅猛发展，使用身份认证和金融支付的媒介越来越多，如银行IC卡(欧美等地称为EMV卡)、网银U盾、电子护照、手机支付、社保卡、身份证等。侧信道分析技术因此备受关注、发展迅速，应用范围日益广泛。学术界和工业界已报道的被破解的算法包括多种通用对称算法、公开密钥算法，被破解的设备类型包括含专用芯片(ASIC)的智能卡、电子护照芯片、网络通信安全套接层加密芯片，甚至云计算虚拟机等。

以中国金融电子支付为例，10年间从磁条存折、磁条卡、网银U盾到如今的手机近场支付、手机网银等，技术发展的浪潮方兴未艾。日前值得关注的一大热点是互联网金融新模式，既不同于商业银行间接融资，也不同于资本市场直接融资。关于交易媒介、计价单位、价值储藏等方面的技术革新可能即将到来。例如，目前以密码算法为安全基础的支付终端是否将与后台征信数据交互，形成实时违约数据；目前金融支付等在中央银行支付清算系统下进行，将来网络社区内的支付活动能否进一步与股票、债券、存贷款、信用透支等融合，产生新兴业务，这会对身份认证(匿名实名)、系统安全产生何种影响。这样迅猛发展的电子支付或其他相关产业对信息安全需求十分强烈。

侧信道分析攻击技术给商业产品、个人安全应用、国家军事安全带来了实际的威胁。目前大多数密码集成电路产品所能采用的安全措施是有限的，一方面受成本制约，另一方面也有保护方法研究不成熟的原因。在我国大力发展金融安全和基于个人身份信息征信系统的时代，希望本书能提供给读者侧信道分析技术的基础知识和对未来发展的展望。

国外同类书籍大多只讲述功耗攻击(侧信道攻击的一种)，本书系统讲述侧信道技术和密码安全芯片设计中的侧信道防御技术以及安全评估技术。目前国内还没有侧信道技术的相关书籍面世，希望本书的出版能够方便我国读者了解侧信道技术，同时抛砖引玉，带动我国更多专家学者共同努力，提升侧信道或者更广泛的芯片攻击防御技术。

本书的出版得到了国家863计划项目(2007AA01Z459)、国家科技重大专项(2009ZX02038)、国家自然基金青年基金项目(60901052)和其他一些省市科技项目

资助，书中的许多理论分析和数据是在上述研究过程中产生的。特别感谢各位老师、同事、学生等多年来的帮助，书中的一些实验和分析由陈廷定、邬可可及国民技术股份有限公司、商用密码检测中心承担国家863计划项目(2007AA01Z459)的相关人员共同完成。部分算法知识是在与信息安全国家重点实验室的学者讨论过程中获得的，部分光致错误攻击技术是在与英国剑桥大学信息安全实验室的学者讨论过程中获得的，部分侵入式攻击、错误分析攻击等技术是在与银行卡检测中心的技术人员讨论过程中获得的。CHES(Workshop on Cryptographic Hardware and Embedded Systems)会议中众多学者的闪光思想也给作者许多灵感。在此一并表示衷心的感谢。

由于国内外信息安全技术与集成电子技术发展迅猛，侧信道分析技术研究和应用的侧重点也在不断变化，例如，侧信道功耗分析与选择明文攻击的叠加、故障分析与功耗分析的叠加以及近年来日益受到关注的硬件木马等，因此本书未能面面俱到。加上本书作者水平有限，书中的不足之处在所难免，还请读者不吝赐教。

作 者

2013年4月

目　录

第 1 章　信息安全简介

1.1　信息安全基础知识

假定发送者想发送消息给接收者，且希望安全地发送信息，接收者希望安全地接收信息，有四个基本的安全特性必须得到满足：机密性(confidentiality)、完整性(integrity)、不可否认性(non-repudiation)、身份确定性(authenticity)。

机密性：保证窃听者不能阅读发送的信息。

完整性：消息的接收者能验证在传送过程中消息没有被修改；入侵者不可能用假消息代替合法消息。

不可否认性：发送者事后不可能虚假地否认他发送的消息。

身份确定性：消息交互双方应该能够确认对方的身份；入侵者不可能伪装成他人。

消息(message)一般称为明文(plaintext)。用某种方法伪装消息以隐藏其内容的过程称为加密(encryption)，被加密的消息称为密文(ciphertext)，而把密文转变为明文的过程称为解密(decryption)[1]，图1.1展示了这个过程。

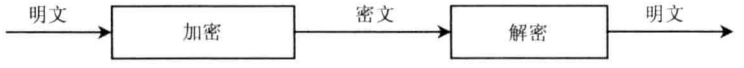


图 1.1　加密和解密

1.2　密码学

密码学包括密码编码学和密码分析学两部分。本书所关注的侧信道分析技术是密码分析学的一个分支，是密码学、电子信息技术的一个交叉。

在计算机出现之前，密码学由基于字符的密码算法构成。不同的密码算法是字符之间互相代替(substitution)或者互相换位(transposition or permutation)。由于计算机和各种电子设备的出现，密码算法变得复杂多了，但是原理还是没变。大多数好的对称密码算法仍然是代替和换位的元素组合。

代替就是明文中每一个字符被替换成密文中的另一个字符。接收者对密文进行逆变换就可以恢复出明文。著名的凯撒(Caesar)密码就是一种简单的代替密码，

它的每一个明文字符都由其右边第三个字母代替(A由D代替，B由E代替，……，W由Z代替，X由A代替)。简单代替密码很容易破译，因为没有掩盖明文的不同字母的出现频率。多字母或多表代替密码相对难破译，然而使用计算机就可以轻易找到代替的多字母或多表，从而轻易破解具有很长周期的代替密码。

在换位密码中，明文的字母保持相同，但顺序被打乱。图1.2显示了一个简单的纵横换位密码。明文以固定的宽度水平地写在一张图表上，然后水平地读出明文。第一次世界大战中，德国人所用的ADFGVX密码就是一种换位密码与简单的代替密码的组合，在那个时代是一个非常复杂的算法，但是被法国密码分析家George Painvin破译。许多现代密码也使用换位，但由于对存储要求很大，代替密码要常用得多。

明文： COMPUTER GRAPHICS MAY BE SLOW BUT AT LEAST IT IS EXPENSIVE

C O M P U T E R G R
A P H I C S M A Y B
E S L O W B U T A T
L E A S T I T I S E
X P E N S I V E

密文： CAELX OPSEP MHLAE PIOSN UCWTS TSBII EMUTV RATIE GYAS RBTE

图 1.2 纵横换位密码

现代密码学由香农(Shannon)创立。1948年香农发表《The communication theory of secrecy system》成为现代密码学的理论基础。1949年香农发表了著名的《信息论》，1950年又发表了《保密系统的通信理论》，首次将密码学研究置于坚实的数学基础上，建立了密码学的理论基础，证明了一次一密(one time pad)的密码系统是完善保密的(perfect secrecy)，促进了流密码的研究和应用。一次一密的密钥是不重复的真随机数，每个密钥仅使用一次。发送者对所发送的消息加密后，销毁密码本用过的部分。接收者有一个同样的密码本，并使用对应的密钥解密密文，解密后也销毁密码本用过的部分。香农的论文还提出了分组密码设计应该遵循的准则，如扩散和混淆，并证明了消息冗余使得密码破译者统计分析成功的理论值(唯一解距离)。这些理论至今仍然是密码学的基础。

1.2.1 对称加密与公钥加密

实现信息安全四个基本特性的重要手段是加密、签名。目前加密算法中，对称加密是最广泛使用的加密方法，也称为常规加密，使用一个循环结构迭代加密，在该循环中重复置换和替换输入数据。对称加密中加密密钥和解密密钥是同一个

密码，称为K，如图1.3所示。三种国际上常用的对称加解密算法是数据加密标准(data encryption standard，DES)、三重DES (triple DES，3DES)和高级加密标准(advanced encryption standard，AES)。

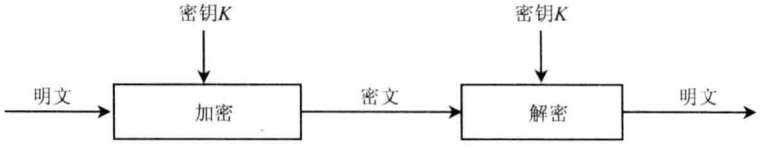


图 1.3　对称加密

在对称加密体系中，欲获得消息安全交互的两个当事人必须拥有同一个密钥，保护该密钥不被其他人得到，而且需要频繁地改变密钥。如果攻击者获得了密钥，更改密钥可以限制被窃数据的数量。所以密钥分配技术是密码系统中非常重要的环节[1,2]。

对于两个当事人A和B，密钥分配技术通常有以下几种：

(1) 由当事人之一选择密钥，然后物理地或者通过加密通道将密钥传递给另一方。

(2) 由第三方C选择密钥，然后物理地或者通过加密通道将密钥传递给A和B。

(3) 使用公钥加密。

公钥加密与对称加密同等重要，它可以用于加密，但更普遍的应用是消息认证和密钥分配。公钥加密由Diffie和Hellman在1976年公开提出，这是密码学史上具有革命意义的进步。公钥加密算法是基于数学函数而不是对位的简单操作。另外，与对称加密相比，公钥加密使用两个不同的密钥，在机密性、密钥分配和认证领域，使用两个密钥具有深远的意义，图1.4是公钥加密体系示意图。

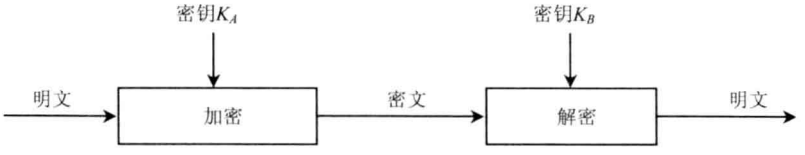


图 1.4　公钥加密

公钥加密方案中有一对密钥，称为公钥和私钥(public and private key)。一个用于加密，一个用于解密。所有的信息交互当事人都能够访问公钥，而私钥则由每个当事人在本地产生，不进行分配。只要用户保护好私钥，通信就是安全的，而且用户可以改变私钥，并公布相应的公钥值以替代旧的公钥值。关于公钥加密，有几个常见的需要澄清的误解：

(1) 从密钥分析的角度，公钥加密比对称加密更加安全。事实上，任何密码

系统的安全性都依赖密钥的长度和破解密钥的计算工作。从抵抗密码分析的角度，目前没有理论证明公钥加密比对称加密更加安全。

(2) 公钥加密是通用的技术，人们少有继续使用对称加密。事实上，公钥加密的计算开销比对称加密大得多，因此在计算资源有限的情况下，对称加密仍是首选。

(3) 在使用公钥加密的时候，与对称加密密钥分配中相当烦琐的握手协议相比，公钥加密的密钥分配不再重要。事实上，公钥加密需要独有的协议(通常会需要一个中央代理)，密钥分配的过程并不简单。

根据具体的应用场景，发送者执行加密函数时，使用的是发送者的私钥或者接收者的公钥，或者两者同时使用。公钥加密系统的应用分为以下几类：

加解密：发送者用接收者的公钥加密消息，如图1.5所示。

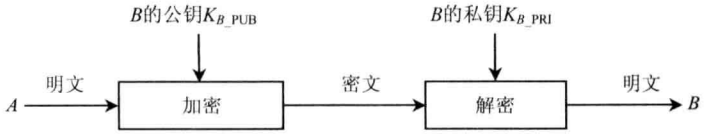


图 1.5 公钥密码应用(加密)

数字签名：发送者用自己的私钥签名消息，如图1.6所示。

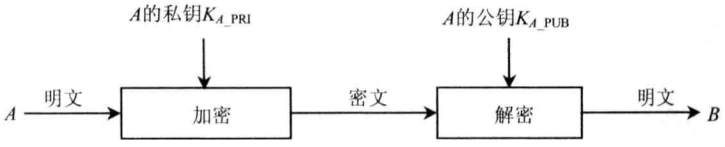


图 1.6 公钥密码应用(签名)

密钥交换：双方合作交换会话密钥，可用多种方法，如使用一方或双方的私钥。

1.2.2 分组密码与流密码

除了按照密钥对称与否对密码算法分类，也可用明文的处理方式对算法分类。如果将明文空间的元素(如字母、二元数字等)逐个加密，称为流密码或者序列密码；如果将明文空间的元素分组(每组含多个元素，如多个字符、一帧图像等)，逐组加密，称为分组密码。

对于流密码，明文字符分别与密钥流作用进行加密，解密时以同步产生的密钥流作解密变换。流密码强度完全依赖密钥流生成器所生成序列的随机性和不可

预测性。如果密钥流是真正的随机数流，则这种体制在理论上是不可破译的，即一次一密，但这种方式所需的密钥量大得惊人。目前一般采用伪随机序列代替随机序列作为密钥序列。伪随机数序列存在着一定的循环周期，如果周期足够长，那么会有较好的保密性。

伪随机数密钥流生成器有多种结构，多数是用线性反馈移位寄存器或非线性反馈移位寄存器作驱动器产生一系列状态序列，这些状态序列经过非线性组合后得到密钥序列。流密码加解密的工作原理非常直观。用密钥序列k对明文序列m进行加密的过程是将k和m对应的分量进行模2相加，得到加密后的密文序列c。在接收端，合法的接收者的解密过程就是将密文序列c和密钥序列k的对应分量进行模2相加，即得到原来的明文序列m。

流密码体制的一个优点是每一比特的密文数据与其他密文比特无关。这样即使一个密文位发生了错误，对整个数据段的影响也不大。流密码加解密速度很快，应用较普遍，如GSM网络中的数据加密算法。但是流密码需要保持收发两端密钥流的精确同步。与流密码相比，分组密码容易实现同步。分组密码的主要缺陷表现在两个方面：一是分组加密不能隐蔽数据模式，即相同的密文组蕴含着相同的明文组；二是分组加密不能抵抗重放、嵌入和删除等攻击。但分组密码的上述缺陷可以通过在加密处理中引入少量的记忆克服。

流密码和分组密码各有优缺点，如何选用应该由具体应用场景决定。

1.2.3　密码算法的保密与密钥的保密

密码算法(algorithm)也叫密码(cipher)，是用于加密和解密的数学函数。如果信息安全性来自算法的保密，那么这种算法称为受限制的(restricted)算法。受限制的算法具有历史意义，但是大的或经常变换的用户组织不能使用这种算法。因为如果有一个用户离开这个组织，其他的用户就必须改换算法，以免有意或无意地将算法泄露。

现代密码学认为安全性应该来自密钥的保密，对于好的加密方法，密钥的秘密性理应足以保障资料的机密性。这个原则于19世纪由柯克霍夫(Kerckhoffs)提出并被称为柯克霍夫原则(Kerckhoffs' principle)。香农重申为“敌人了解系统”。

20世纪，美国国家标准局(National Bureau of Standards，NBS，后更名为美国国家标准技术研究所，National Institute of Standards and Technology，NIST)制订了数字加密标准，Diffie和Hellman发表了公钥算法开创性论文，Rivest、Shamirh和Adlema公开发表了RSA算法。至此，现代密码学成为保障通信、网络、个人电脑安全的重要工具。许多现代密码技术的基础依赖特定计算问题的困难度，如因子分解问题或离散对数问题。所有这些算法的安全性都基于密钥的安全性，而不是

基于算法细节的安全性。这就意味着算法可以公开，被分析，大量传播。现代密码系统(cryptosystem)由算法以及密钥共同组成。

1.3 密码设备

我国信息安全产品(或称密码设备)已经广泛应用于保密传输、网络安全和身份认证等领域，信息安全技术的核心就是对信息进行处理。信息处理技术的核心则是计算机技术，究其根本是密码集成电路技术。现代信息安全对密码集成电路的依赖越来越强，密码集成电路已经成为信息安全所依赖的关键技术之一。基于密码芯片的硬件解决方案已经成为保证信息安全的可靠途径。随着信息化的发展，密码芯片越来越多地出现在各种应用场合。在计算机芯片组、路由器、交换机以及个人设备中的手机、智能卡中，已经或将要实现内置安全控制模块。信息安全芯片目前已逐渐成为国家、个人信息安全基础设施建设的基石。

芯片级的安全解决方案正成为密码设备的重点发展方向。在个人电脑及服务器的安全方面，芯片级的安全产品已经面市，如可信平台模声(trusted platform module，TPM)。新型安全芯片储存了计算机的验证信息，包括计算机的安全、加密和密码管理等信息内容，将这些信息锁定在计算机状态中，保证这些信息不被外部的黑客篡改，从而有效地阻止黑客入侵。在手机等手持无线设备的安全方面，为保护无线网络免受黑客攻击，保障电子商务交易、应用软件下载、游戏和多媒体内容的安全，手机数据安全和用户信息安全的重要性日益凸显，而软件安全的漏洞会导致被盗电话的可重编程、非法升级、网络切换、网络隐患等多种问题，因此芯片级安全方案应运而生，为手持无线设备带来安全计算，提供安全的无线交易。安全芯片将渗透到安全的每一个领域并将成为一种趋势，芯片级安全技术已经成为跨国半导体巨头角逐的一个重点方向，信息安全芯片已成为近年来集成电路产业增长的重要部分。

现代密码学包括不同类型的密码算法。这些密码算法按照一定的密码协议可以构成安全解决方案。但是所有的密码算法都是抽象的数学算法。只有将密码算法以某种形式实现才能形成可用的密码技术或产品。实现密码算法的方式可以分为软件方式和硬件方式。硬件方式又分为嵌入式实现、FPGA芯片实现和专用芯片实现。能够直接实现或支持密码算法实现的硬件称为密码硬件设备，能够直接实现或支持密码算法实现的ASIC芯片称为密码芯片，或信息安全芯片。

密码芯片既然涉及密码算法、密钥等信息安全的关键信息，就必然成为攻击者的目标。攻击者对其进行非法读取、分析、解剖等攻击，以期获得有用信息和非法利益。目前已经发现针对密码安全芯片的多种攻击方法，如超高超低时钟频率攻击、超高超低电源电压攻击、电源能量分析攻击、物理探测攻击等，严重威

胁着密码芯片中密钥及密码算法等机密信息的安全。攻击方法主要有以下几种：

(1) 微探测(microprobing)：通过电子探针或机械探针对芯片进行探测和分析，获取关键信息；另外，聚焦离子束(FIB)可对芯片的连线、存储器等进行物理修改。

(2) 软攻击(soft attack)：通过正常的通信接口，分析和寻找协议、密码算法和应用中的漏洞。

(3) 侦听(eavesdropping)：通过能量分析设备，测量芯片工作时的能量与电磁辐射，然后进行分析与仿真，从而获取内部关键数据。

(4) 故障生成(fault generating)：通过非正常操作，如改变芯片的工作频率或工作电压，使芯片工作异常，实现非法访问，获取信息。

(5) 解剖分析：对芯片显微照相，提取网表，进行功能仿真和综合分析。

(6) 侧信道分析(side-channel analysis，SCA)攻击：通过分析密码芯片的功耗曲线、电磁泄漏、时序等获得芯片中密码算法的密钥。侧信道分析方法可以分为四大类：简单侧信道分析(simple side-channel analysis，SSCA)、差分侧信道分析(differential side-channel analysis，DSCA)、相关性侧信道分析(correlation side-channel analysis，CSCA)和互信息分析(mutual information analysis，MIA)等。

目前尚没有一种完美的方案能彻底解决芯片的安全问题，但是如果能够针对上述实现方法在安全上的弱点建立一系列有效的物理防护手段，就可以在很大程度上解决芯片的安全问题。如果攻击芯片的代价高于攻击者从攻破芯片中获得的回报，攻击行动本身将失去意义。因此，在密码集成电路及IP核的设计中，考虑增加抗击各种攻击的手段和方法是十分重要和必要的。本书将着重讲述安全芯片侧信道分析攻击防御技术。

1.4　侧信道分析技术

侧信道分析攻击(side-channel analysis attack)技术是相对于传统意义上基于通信的密码分析而言的。传统的密码分析是通过对密码处理器的算法进行破解分析，并对输入输出等数据辅之以监听等手段，在流程内实现攻击。侧信道分析攻击技术的对象则是密码处理器的实现，即不是对加解密数据本身分析，而是对加解密过程中的时序、功耗等其他信道的信息进行分析，从而得到密钥等敏感信息。图1.7显示了以智能卡芯片为例的侧信道分析方式。

与传统的密码分析(cryptanalysis)相比，侧信道分析攻击技术具有成本上的优势。密码分析虽然通过一些分析方法可以降低密码破解的强度，即缩小穷举

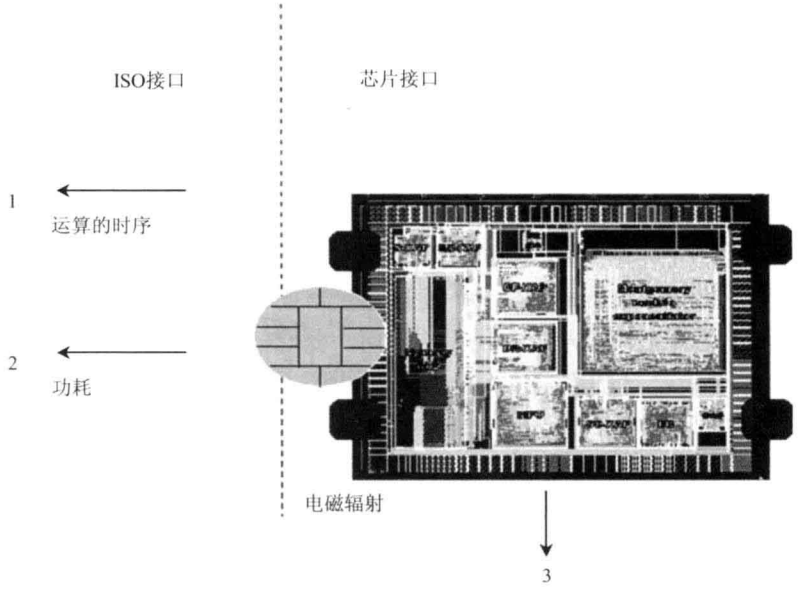


图 1.7 侧信道分析

密钥的空间，但是目前通常采取的延长密钥位的办法可以使实现穷举攻击需要的时间远远长于密钥的生存期。侧信道分析攻击技术的破解效率与密钥长度无关或只是线性相关，而非传统密码分析中，其效率与密钥长度的幂相关。如果集成电路未采取保护措施，则侧信道分析攻击技术可能只需要很小的代价就可以获得密钥。例如，功耗分析通常只需要数千美元的成本，根据现有的文献资料，如未对侧信道攻击进行防御设计，许多算法可在短期内(几分钟到数天)被破解。因此，侧信道分析攻击技术成为破解密码芯片的一条“捷径”，越来越受到学术界和工业界的关注。

随着信息安全日益受到人们关注，密码集成电路的攻击方法得到了比较广泛而深入的研究，而且也给商业产品带来了实际的安全威胁。目前大多数密码集成电路产品所能采用的安全措施是有限的，其中有成本因素，也有保护方法不成熟等原因。但是攻击方法也不是万能的，表现在以下几个方面：

(1) 目前的攻击仍然集中在以智能卡为代表的资源受限的一类密码集成电路。

(2) 许多攻击方法依赖算法实现或防御方法的细节，在大部分资源受限、专业技术受限的攻击中是有难度的。

(3) 集成电路工艺水平的提高使得攻击的难度不断增大。例如，反向工程(reverse engineering)在深亚微米工艺条件下越来越困难。

参 考 文 献

[1] Schneier B. 应用密码学——协议、算法与 C 源程序. 吴世忠, 等, 译. 北京: 机械工业出版社, 2000.

[2] Stallings W. 网络安全基础——应用与标准. 2 版. 北京: 中国电力出版社, 2004.