

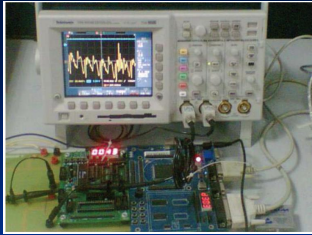
目录	
旁路攻击 SCA 及防御	3
密码攻击	4
数学攻击	5
实体攻击	6
微探针技术	7
版图重构	8
实现攻击	9
主动式攻击（失效分析攻击）	11
干扰攻击	13
电涌攻击	15
电磁攻击	16
光攻击	19
热攻击	22
射线攻击	23
被动式攻击（旁路攻击SCA）	24
条件	28
攻击过程	28
机理	29
CMOS电路的瞬间物理功耗模型	30
旁路攻击原理	32
旁路攻击分类	33
时间攻击	34
故障攻击	35
功耗攻击	36
电磁攻击	37
声音攻击	38
可见光攻击	39
组合分析攻击	40
旁路攻击分析技术	41
对旁路攻击的防御技术	42
已有的抗攻击研究	43
算法级	43
电路级	44
软件算法抗攻击研究	45

1

对旁路攻击的硬件防御技术	46
反向调节技术	47
乱序技术	48
间接供应电源技术	49
并行处理器技术	50
异步电路技术	51
冗余编码技术	52
掩码技术	53
对旁路攻击的硬件防御方法	54
对旁路攻击的软件防御技术	56
数据冗余	57
控制冗余	58
执行冗余	59
对旁路攻击的软件防御实现方法	60

2

旁路攻击 SCA 及防御



传统思想路线忽视

功耗泄漏、电磁泄漏、执行时间等

输入信道(明文) → 密钥处理 (加/解密、签名、认证等) → 输出信道(密文)

密码芯片

3

密码攻击

- 对加密算法的攻击大体可分为**数学攻击**、**实体攻击**、**实现攻击**等。
- 实体攻击需要**昂贵**的高端实验室设备和专门的探测技术，实施起来具有一定的难度；应对实体攻击的关键在于提高芯片设计的复杂程度和芯片制造的精细程度。
- 实现攻击并不需要打开密码模块或密码系统的硬件封装，因此是一种相对廉价与相当有效的攻击方式。与传统的数学分析方法相比，**实现攻击**具有**较小的密钥搜索空间和较高的分析效率**。

4

密码攻击-数学攻击

- 数学攻击：是以**线性攻击**和**差分攻击**为代表的传统密码分析方法，利用加密算法的统计特性，通过分析选择的明密文对来获取密钥。**实施这类攻击往往需要俘获和处理异常巨大的数据量，在现实中并不总是可行。**

5

密码攻击-实体攻击

- 实体攻击主要是通过去除芯片或电路的封装，观察、操纵和干预系统内部芯片的某些点的状态及芯片与外围电路之间的通讯来获得信息；改变电路结构；直接获取存储器数据等。

6

实体攻击方法之一

- (1) **微探针技术**：攻击者通常在去除芯片封装之后，通过恢复芯片功能焊盘与外界的电气连接，最后可以使用微探针获取感兴趣的信号，从而分析出电路的有关设计信息和存储结构，甚至直接读取存储器中的信息进行分析。

7

实体攻击方法之二

- (2) **版图重构**：利用高倍光学及射电显微镜研究电路的连接模式，可以迅速识别芯片上的一些基本结构，如数据线、地址线、控制线、RNG等。其结果是存储内容被攻击者非法获得，旁路某些敏感电路。

8

密码攻击-实现攻击

- 实现攻击：加密算法的实现电路经常会泄漏一些有用信息，这些信息能够被用来分析加密算法的敏感数据或密钥，这即是实现攻击。
- 实现攻击可分为主动式攻击（失效分析攻击）和被动式攻击（旁路攻击）

9

实现攻击使密码系统设计陷入困境

- 因为用以往我们保护分组密码的技术来对付实现攻击效果将适得其反。比如，以往我们采用尽量长的密钥来保证分组密码系统的安全，但是长密钥带来的就是长时间的运算操作，这使得实现攻击根据时间分析来获得更多的关于密码系统的信息。因此也许我们应该改变设计密码系统的方法。

10

实现攻击-主动式攻击

- 主动式攻击是一种侵入式攻击，通过引入故意错误如数据抖动、电源或时钟突变来影响加密电路的正常运算过程，从而分析出密钥。
- 在主动式攻击中，攻击者通过将芯片放置于异常物理环境中有意使得芯片指令的执行出现故障或错误。干扰式攻击通常用来将芯片关键指令的执行替换成任意其他指令的执行，也可以用来在数据传递于寄存器和存储器间时更改传输数据。

11

实现攻击-主动式攻击

- 目前已知的干扰方式有时钟信号短暂扰动，电源供应短暂扰动，外部电磁场短暂扰动等；还有光、温度、射线等扰动；
- 时钟信号扰动是目前最容易和有效的干扰方式。

12

干扰攻击目的

- 回避某些判断、跳转指令的执行，从而**逃避安全检查**，例如认证等；
- 降低时钟频率可以**更容易的采集信息**，从而提高获取敏感数据的可能性；
- 使CPU执行**非法指令可能引起非法的地址访问**，从而泄露芯片中的安全信息；
- 简短程序循环的次数，比如**减少密码运算的轮运算**，使得算法更易攻击。

13

干扰攻击机理

- 瞬间扰动可以应用在时钟信号或电源信号上，因为不同信号路径的逻辑门数目不同，**延迟就不同**，通过改变扰动的精确时间和长度，可以**导致处理器执行错误或非法指令**。例如：
- 高频时钟可导致处理器没有足够的时间将跳转地址写入程序计数器而使得**程序分支跳转无法执行**；
- 高频时钟与时钟毛刺的效果是一样的，可对CPU的译码和指令执行产生影响，导致CPU执行非法指令；
- 非正常的电压会影响**NVRAM的写入特性**；
- 非正常的电压会引起**RNG的不正常工作**，使随机数输出不随机，还可能使CPU执行非法指令。
- 时间和功耗分析可以用来在扰动中监视程序走到哪一步，以辅助扰动的效果。

14

失效分析攻击--电涌攻击

- (1)尖峰电涌攻击
在多种失效分析攻击方法中，多年来最简单、应用最广泛的方法就是修改智能卡控制器的信号输入或供电。目前市场上广泛存在的卫星电视黑卡就是用这种方法破解的。供电中的瞬时能量脉冲被称为电涌Spike；所谓的Glitch尖峰脉冲则被定义为对时钟信号的特别修改。由于电源和时钟信号都是芯片运行的必需条件，尖峰和电涌攻击都会导致芯片控制器故障，即某些电子模块会暂时失效，因此会跳过或实施错误的操作。

15

失效分析攻击--电磁攻击

- (2)电磁攻击
虽然尖峰和电涌攻击能够得到一些效果，更复杂的方法已经能把电压和信号的改变融合进半导体芯片中。例如，对GSM SIM卡的PIN码攻击可以使攻击者完全不需懂得PIN码的知识就能分析出卡中的保护数据。为了把扰乱的信号注入芯片，经常使用电磁线圈，需要把它直接放到芯片表面。电磁攻击虽然更复杂，但比起传统的尖峰或电涌攻击方法来，一个明显的进步是可以把芯片放在一个特殊的模块上进行本地的攻击。这就导致相应的防范策略更难被开发。一个安全控制器可以监视它的外部供电压，可以监测到一些尖峰和电涌，但是如果一个电磁脉冲被加到一个专门的模块上，例如加密协处理器，就很难被监测出。

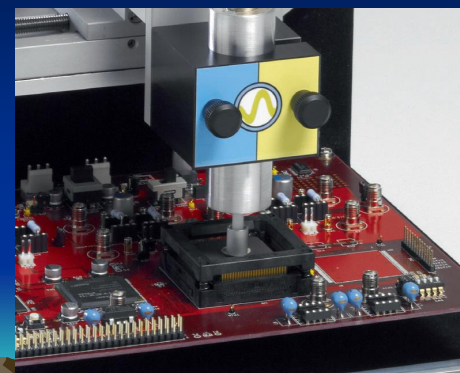
16

电磁攻击



17

电磁攻击



18

失效分析攻击--光攻击

• (3) 光攻击

光攻击是指用光照射正在工作的安全控制器表面，由于光的入侵，芯片的硅片内部会产生电压和电流，从而导致失效行为。采用这种技术的攻击者可以绕过密码或PIN码，而得到私密数据；或者对加密操作进行攻击从而产生密钥数据。分为全局光攻击和局部光攻击。这种攻击需要很强的光照，这就意味着需要用到闪光灯或激光。任何芯片覆盖层都不能提供有意义的屏障。

19

光攻击



20

光攻击



21

失效分析攻击--热攻击

• (4) 热攻击

修改环境温度也可被用作对安全控制器的攻击方法。通过增加周边环境的温度，RAM内存的一些位会被修改，这种方法可被用来攻击各种虚拟机架构。相反，降低温度也可用来进行攻击——极低的温度可以导致RAM中存储信息的冻结，即便是外部供电已被关闭。温度攻击用于安全芯片的有效性很大程度上取决于芯片采用哪种内存类型。一般应对热攻击的对策在芯片上加装温度传感器，如果温度超过界限，则发出警报。

22

失效分析攻击-- 射线攻击

• (5) 射线攻击

对芯片用Alpha射线照射已成为及其简单且有效的攻击，但这种攻击方法仍存在一些局限性。采用Alpha射线，攻击者将不能够预测失效发生的确切时刻，也就是说，这种攻击纯属统计过程。对Alpha射线的聚焦并不容易。必需通过对多次失效结果的纪录，然后进行后期的分析。这导致攻击的实时性不好。已知的Alpha射线攻击的效果包括对内存内容的更改和信号时序的延迟等。因为不需要昂贵的设备，用Alpha射线的攻击对某些应用是很危险的。Alpha攻击的成功主要取决于攻击者的经验和特别对芯片内部的了解。

23

实现攻击-被动式攻击

- 被动式攻击也旁路攻击 SCA (side channel attack)，它是指加密系统能够以各种形式泄漏信息，比如温度、声波、能量耗散、执行时间、电磁泄漏和光信号等，通过提取加密电路中的泄漏物理量，分析泄漏物理量变化规律来从而分析出密钥。
- 旁道攻击是一种针对密码设备的新型攻击技术。研究人员于1996-1999年间开始进行关于旁道攻击的研究。
- 旁道攻击不同于传统经典的、专注于数学理论而对密码系统进行研究的方式，而是一种针对密码系统实现上的物理攻击方式。但它既没有系统的攻击方式，也没有系统的解决方法。

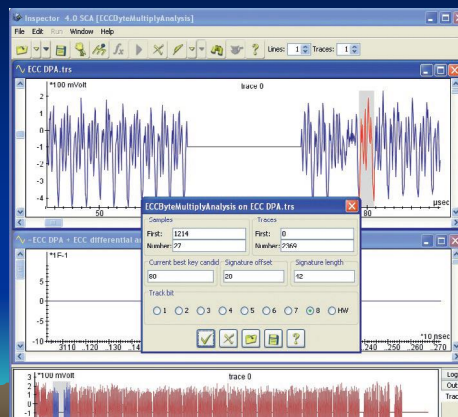
24

旁路攻击



25

旁路攻击



26

实现攻击-被动式攻击

- 利用电磁辐射的**电磁攻击方法**和利用能量消耗的**能量攻击方法**是两种非常有效的旁道攻击方法，也是目前旁道攻击的热点；
- 电磁信号的噪声比能量信号的噪声小，保留了泄露的秘密密钥的模式，而能量信号暴露了芯片在该位置的的电位差，所以电磁攻击和能量攻击这两种攻击方法可以互相补充，有时可以联合使用。

27

实现攻击-被动式攻击

- 旁路攻击是基于统计理论的物理攻击方法。
- 旁路攻击的必要条件：
 - 一、有**足够多的采样样本**；
 - 二、各密钥相关状态的**准确采样值**。
- 攻击过程可以分为2个阶段：
 - 一、泄露信息的**采集阶段**
 - 二、密钥**分析**阶段。

28

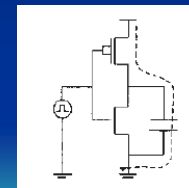
旁路攻击机理

- 集成电路的核心技术即为CMOS技术。CMOS电路是由上拉P-MOS管和下拉N-MOS管电路构成，PN结是互补的。
- 当输入电流稳定，只有一个结导通；
- 当数据发生变化时，反映在CMOS电路上即为状态的变化，这种状态的变化导致CMOS电路的功率消耗（**电路的瞬间物理功耗模型见下页**）。
- 通过仪器可以测量到变化。

29

CMOS电路的瞬间物理功耗模型

- 门电路的功耗是以下三种类型功耗的和：
- (1) **泄漏电流功耗**，就整体功耗来说是很小的；
- (2) **对电容CL充电放电的动态功耗**，为主要功耗。
- (3) 发生0到1转换时从源到地的**短路电流功耗**，大约占整体功耗的15-20%；
- 倒相器的动态功耗Pm表达式为：
$$P_{dyn} = C_L * V_{DD}^2 * P_{0 \rightarrow 1} * f$$
- 其中Pdyn为0、1转换的功率
- f为设备的工作频率
- VDD为电源电压
- CL为电路中的电容



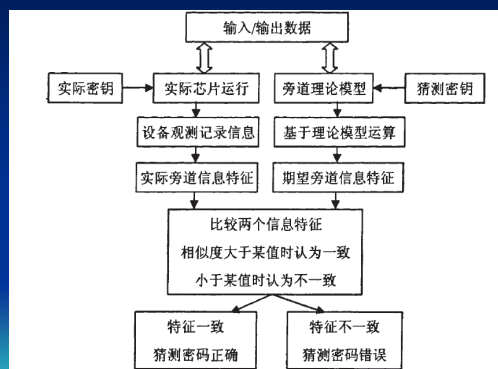
30

CMOS电路的瞬间物理功耗模型

- 如果CMOS门改变了状态，这种改变可以监测到。变更状态的电路越多，耗散的功率越大。在同步设计中，所有门电路在同一时刻改变其状态。每个门的输出均有一个由引线产生的寄生电容和下一级门电路构成的容性负载。输入端的变化导致了输出端的变化，从而对寄生电容进行充放电，引起电源端电流流动和电磁辐射。
- 在一个特定的时间 t ，电路的功耗和辐射是同一时刻所有门电路的功耗和辐射的和。

31

旁路攻击原理



32

旁路攻击分类

目前已经发现且被证实有效的旁路泄漏信息有多种，按泄漏特征进行划分，旁路攻击可以分为以下几类：

- (1) 时间攻击 (Timing Attack)
- (2) 故障攻击 (Fault Attack)
- (3) 功耗攻击 (Power Attack)
- (4) 电磁攻击 (Electromagnetic Attack)
- (5) 声音攻击 (Acoustic Attack)
- (6) 可见光攻击 (Visible Light Attack)
- (7) 组合分析攻击
- 在诸多旁路攻击手段中，**能量攻击和电磁攻击最为强大和高效**，目前的研究工作主要是对这两种攻击方法。

33

旁路攻击之一 -----时间攻击

- 1996年美国科学家Paul首先发现针对密码芯片的时间攻击法。该方法通过对密码芯片运算过程中执行时间信息的采集，结合密码算法的内部实现，证实了算法指令和执行时间存在相关性，从而推测出密钥信息。在Paul的基础上，Dhem等人将时间攻击方法成功地应用于破解RSA密码算法。

34

旁路攻击之二-----故障攻击

- 故障攻击是1996年由Boneh等人首次提出的对RSA公钥密码体制的新型攻击方法。该方法利用密码计算过程中的故障信息来破解密码系统。1997年Biham和Shamir将这种攻击方法应用于对称密码体制，首次提出“差分故障攻击”的概念，并成功地攻击了DES算法。此后，研究人员提出各种不同的故障攻击方法，成功地攻击了多种密码体制，如ECC、AES、3DES等。

35

旁路攻击之三-----功耗攻击

- 功耗攻击是一种利用密码设备运行时的功耗泄露信息来推测密码系统所进行的操作和秘密信息的攻击方法。功耗攻击已经被用于破解几乎所有的对称密码和公钥密码，Paul声称仅需要数十条功耗泄漏曲线，就可以在几分钟内迅速地破解没有防御措施的大多数智能卡。

36

旁路攻击之四----电磁攻击

- 2001年, Gandolfi等人提出了电磁攻击方法。2002年Dakshi对电磁泄露攻击进行了系统深入的研究, 并指出电磁泄露的信息非常大, 其攻击方法比时间攻击和能量攻击更为有效, 电磁攻击不仅可以与能量攻击相媲美, 而且对于某些能量攻击无法破解的系统, 电磁攻击也能够破解。

37

旁路攻击之五----声音攻击

- 声音攻击的研究主要是由以色列Weizmann科学研究院的科学家Adi Shamir和Eran Tromer开展的。从理论上说, 主板上电容器发出的声音能提供一定的解密线索, 其泄漏方式与电磁泄漏或者能量波动十分相似。Shamir发现PC机运行时产生的声音信息量十分惊人, 由于电容器发出的音频信号高于风扇产生的频率, 所以很容易将其过滤出来并用作密码分析。2005年, Shamir等人通过上述方法证实了处理器运算时的声音泄露和所执行的操作之间存在相关性。例如, 研究人员发现对于不同的密钥, RSA signature / decryption的声音是不同的, 通过观察音频信号则可以重现密码操作的时间序列, 并可以为时间攻击 (Timing Attack) 提供有价值的信息。

38

旁路攻击之六----可见光攻击

- Kuhn的研究工作表明CRT显示器散射出的可见光可以用于重新构建CRT显示器上的信息。可见光攻击不同于时间攻击和功耗攻击, 该攻击方法不需要和被测的物理设备进行连接, 因此更容易被攻击者使用。Loughry则将该攻击方法应用于LED状态显示器件的攻击。

39

旁路攻击之七----组合分析攻击

- 组合分析攻击: 将功耗分析、电磁辐射分析、时间攻击、故障攻击等方法组合使用, 组合攻击往往比单一途径的分析方法更加有效。

40

旁路攻击分析技术

旁路攻击是基于物理特征的技术, 包括: 故障分析技术、侵入分析技术、时间分析技术、简单功耗分析技术、差分功耗分析技术、电磁辐射分析技术、高阶差分分析技术和汉明差分分析技术、模板分析技术 (template attack)。

模板攻击根据密码设备泄漏旁路信息的数据相关性和操作相关性进行攻击, 首先为密钥空间中所有的密钥分别构建一个泄漏信息特征的模板, 之后根据获取的一份或多份泄漏的信息寻找最匹配的模板, 进而推断最可能的正确密钥或有效缩小密钥搜索空间

41

对旁路攻击的防御技术

- 防御立足点就是破坏旁路功耗分析的两个必要条件:
- 一是消除密码算法实现中信息的泄露;
- 二是增加攻击的难度, 又分为两种:
 - (1) 增加噪声;
 - (2) 减小有效信息量。
- 为了深入地分析旁路泄漏, Micali给出了关于旁路信息泄漏的几条公理:
- 公理1: 计算并且只有计算才能产生泄漏信息。
- 公理2: 相同的计算在不同的计算机上泄漏的信息不同。
- 公理3: 信息泄漏与选择的测量方法密切相关。
- 公理4: 所有的旁路泄漏信息都与计算机内部配置相关。

42

已有的抗攻击研究

- 已有的抗攻击研究主要可以分为**算法级**和**电路级**。现有的比较有效的方法是算法级掩码和电路级的双轨和掩码技术。
- **算法级**最为普遍：这一层次的抗攻击方案主要是利用**掩盖技术**。其通过引入芯片内部产生的随机数对芯片内部的数据进行掩盖，使得电路的功耗、运行时间以及电磁辐射等可探测的因素与运算数据无关。
- **电路级**抗攻击方法：这一级的解决方案是**将电路自身设计成没有旁路泄漏的单元来构建安全芯片**。最近又有一些研究人员从物理以及制造等角度对抗攻击实现进行研究。其中Philips 研究实验室的研究人员从芯片制造的角度找到了一种抗攻击方案。

43

电路级抗攻击研究

- 目前电路级的安全措施主要利用了3个技术：**互补电路**、**电路级Masking**、以及**预充电**。比较有代表性的安全电路有：RSL (Random Switching Logic)、WDDL (Wave Dynamic Differential Logic) 以及MDPL (Masked Dual-rail Pre-charge Logic)
- 1. **利用噪声发生器产生随机的噪声**，加入到可能会被攻击的信号端，以降低功耗分析的信噪比，从而使得功耗分析的攻击方法变得更加困难。但是该方法存在一些缺陷，攻击者可以通过更多的采样和信号处理等方法完成对硬件的攻击。
 - 2. **异步电路**由于其在平均功耗、能量信号的峰值以及电磁辐射等方面的优势，使得它在抵御功耗分析方面也有作用，但由于芯片设计中异步电路本身运用的不是很广泛，相关的设计软件也不是很齐全，这为异步电路在安全芯片中的应用带来了不小的麻烦。
 - 3. **双轨技术**通过加入一个互补电路，平衡了逻辑0 和逻辑1 的功耗，从而破坏了第一个必要条件；而掩码技术通过内部引入随机数，使得内部数据也具有随机特性，从而破坏了第二个必要条件。

44

软件算法抗攻击研究

- 在软件算法对策方面，已经出现几种防功耗分析的方法：
- 1. 增加随机指令如空操作指令的方法来改变密码算法运行程序的时间点，增加采样的难度，从而达到抵御功耗分析的目的。使用亚元变量的方案，可使对于一般变量的赋值变得随机化，真实数据的读取要依据亚元的值而获得。上述的**加入随机指令和使用亚元变量的方法是一类时间随机化的方案**，该类方法虽然增加了功耗分析的难度，但是设计者还要采取必要的措施以防这种随机化不被消除掉。
- 2. 对密码系统中敏感的数据或地址总线进行**位置置换**，以使攻击者不容易得到相关信息。但是攻击者还是可以想办法消除位置置换对功耗分析带来的影响。
- 3. **数据Masking 技术**，即用冗余方式来平衡地表达数据，使得数据的汉明重量恒定，从而攻击者无法得到数据线上泄漏的功耗信息。这种方法具有很好的性能，但是**针对不同的密码算法如何应用该技术，还有许多问题亟待研究**。

45

对旁路攻击的硬件防御技术

- 反向调节技术
- 乱序技术
- 间接供应电源技术
- 并行处理器技术
- 异步电路技术
- 冗余编码技术
- 掩码技术

46

反向调节技术

- 一是通过**增加噪声源**来提升噪声的信号以防止攻击，使攻击者无法区分有信号意义的间峰脉冲和无用的噪声信号。**降低信噪比可以有限地增加一些安全性，增加噪音对防范差分功耗分析基本是无效的。**
- 另一种方案是减少信号幅度，比如使用常量执行路径代码，选择电源消耗较少的缺陷小的操作，使用设备物理屏蔽。

47

乱序技术

- 早期和增加噪音类似的一个办法是在加密实现的代码中打乱某些代码的顺序，**提高分析的难度**。对于这种防范措施，SPA 只要经过仔细的分析处理就可以克服，而DPA 只需要观察有无尖峰，并不在乎尖峰出现在什么位置上，因此基本不受影响（当然需要观察的曲线的时间范围会比原来增大一些）。于是使用**乱序的方法对DPA 而言也基本无效。**
- **关键是代码分块的粒度粗细和等价实现的数量。**

48

间接供应电源技术

- 使用两个电容作为电源器件来支持运行。一半时间电容1 被外部电源充电，电容2 放电来支持芯片工作。另一半时间两个电容做相反的工作。任何时刻IC都会在一个电容的保护下，外部电源从不会直接连到内部芯片，隐藏能耗与密钥的关系。
- 这种方式将给攻击者提取信号带来很大的困难。

49

并行处理器技术

- 就是在IC上增加一个协同处理器，它包含一个可触发的伪随机数产生器，它将和另一个处理器并行工作。当IC要求被校验输入时，协作处理器被以当前值初始化。检测器会检查协作处理器块中的逻辑0 和逻辑1，当为逻辑0 时伪随机序列产生器将产生无用信号来填充当前电源供应。另外，如果是逻辑1，CPU 要求存储内存中的值并开始以无效的垃圾数据显示给攻击者。这种方式将给攻击者提取信号带来很大的困难。

50

异步电路技术

- 在同步电路中功耗的变化随着时钟变化有显著的特性，功耗分析时很容易进行时钟的对准。大量的CMOS 在同一时刻发生翻转变化的，因此功耗的叠加相当明显。
- 在该电路中没有同步时钟信号，通过异步进行信号传输。
- 由于缺少了时钟的参考，指令的执行时间不固定，难以找出特定指令的执行周期。时间上不对齐导致难以取得有意义的功耗平均曲线并作减法，这给DPA 分析带来困难。
- 这个方法实现起来困难较大，不是一个经济的处理方法，且它不是一个数学上可以杜绝功耗攻击的办法。

51

冗余编码技术

- 是指对芯片内部的存储信号进行重新编码，比如比特“0”用“01”表示，而比特“1”用“10”表示，从比特0 变化到比特1 和从比特1 变化到比特0 的信号变化都相同，因此难以区分汉明码重和比特反转引起的功耗变化。这个方法在理论上相对而言比较完善。从硬件实现上，要将电路做成对称的双轨电路。有一条线传输0，就有它的对称线传输1，而实际中只使用其中一条线上的信号。
- 缺点是资源消耗比较大，面积上增加一倍以上；硬件实现上没有相应的自动化设计工具支持。

52

掩码技术

- DPA 攻击需要根据已知的明文和未知的猜测的密钥来推断它们的函数——中间的某个数据。只有当攻击者可以正确推测出中间数据时他才能做出有意义的分类以及进行其后的数据处理。
- Mask 的核心思想就是掩盖中间过程值，加密之前给真实数据加上一个随机数字，中间处理的所有步骤中都有随机数存在，到了最终数据给出前才把这个随机数去掉。
- Mask 比较普遍采用的是将原始数据与一个等长度的随机数异或。
- 利用掩码(Masking)技术平衡地表达数据，使得数据的汉明码重恒定，从而消除数据与功耗之间的相关性。

53

对旁路攻击的硬件防御方法

基于硬件的防护通常包括：

- 时钟的随机化；
- 功耗随机化和功耗平衡；
- 对指令集的运行和寄存器操作随机化等。

54

对旁路攻击的软件防御

- 使用软件方法应对硬件攻击的关键就是要看到：
任何硬件攻击都不能随意改变硬件自身的运行方式，这也是“软件防御”思想的基本内涵。

55

对旁路攻击的软件防御技术

- 数据冗余
- 控制冗余
- 执行冗余
- 特定加密算法的安全实现

56

软件防御技术之数据冗余

- 为防止硬件攻击行为修改存储体上的静态数据和程序代码，可以在存储数据(及程序代码)的时候增加一定长度的冗余数据，用来保证数据的完整性。一种简单的方法就是在每组数据的后面增加循环冗余码。如果对于数据完整性有着更加严格的要求，可以采用一个简单的哈希函数计算出每组数据的杂凑值。通过数据冗余，还可以有效地防止主动攻击对关键数据的修改(比如安全位、指令下载控制位等)，并且由于仅仅是对数据存储格式的变化，这种措施可以在不影响程序结构的情况下，加固安全性。

57

软件防御技术之控制冗余

- 针对对静态数据或者关键代码的篡改，我们可以通过数据冗余的方法进行有效的防御。但是，在程序的动态执行过程中，数据冗余策略就无能为力了，因此还必须增加程序执行时控制的冗余。控制冗余的主要思想就是在包含有关键代码的函数中添加多重控制，以最大程度上保证程序执行是处于完全安全、可信的环境之中。比如，设置多个状态位，在程序的执行过程中不断检查这些状态位的状态，如果有一个发生了改变，程序马上退出执行。

58

软件防御技术之执行冗余

- 对密码算法中独立的(逻辑上没有继承关系、时间上没有先后关系)代码段按随机顺序执行；
- 对同一个功能构造多个不同但是等价的实现随机选择执行；旁路算子
- 随机延时和随机功耗插入；
- 未用资源的随机介入；
- SLEEP的介入；
- 平衡内部数据的汉明重量；
- 做内部数据比特组的分隔；
- 数据单元的等价实现、同步及随机访问；

59

对旁路攻击的软件防御实现方法

- 降低功耗信号抵抗差分功耗攻击：
- 使用固定运行路径的代码；
- 选择功耗旁路中泄漏信息比较少的操作；
- 平衡汉明重量和状态迁移。
- 这类技术往往不能完全阻止功耗信息的泄漏，因为攻击者可以加大功耗信息的采样量使得差分功耗攻击得以进行。

60

对旁路攻击的软件防御实现方法

引入噪声：可以使分析需要异常大量的旁路信息采样。但是噪声本身只能使得差分功耗攻击所需的采样量加大，而如果能够使得成功的差分功耗攻击所需的采样量大到难以采集，则可以有效抵抗这类攻击。

- 将指令运行时间和顺序随机化；加入随机运算可以使得差分功耗分析中的功耗频谱差异难以确定。
- 但是随机噪声总是服从一定的概率分布，攻击者可以借助现代信号处理技术尽可能的滤除噪声，随着数字信号处理技术的发展，常规随机噪声可以通过模式识别、白适应滤波、小波分析等技术手段滤除。
- **如何抵御滤除噪声是关键。**

61

对旁路攻击的软件防御实现方法

- **数据封装技术（MASK技术/掩码技术）**：用冗余方式来平衡地表达数据，使得数据的汉明重量恒定，从而攻击者无法得到泄漏的信息，具有很好的性能，但是针对不同的密码算法如何应用该技术还有许多问题亟待研究。
- 原理：在开始时将信息和密钥以随机方式封装起来，在特定运算点能够将封装拆封，算术掩码和布尔掩码是两种最常用的掩码手段。**要注意乘法掩码0值攻击问题。**
- 例如在运行密码算法前先将算法的密钥进行哈希变换；在公钥密码运算中累加使用指数和模变更处理。
- **算法设计更改或封装技术可以有效抵御差分功耗攻击，但其代价是设计的更改可能导致协议更改或算法与协议不吻合，使得最终产品与标准反而不一致。**

62

