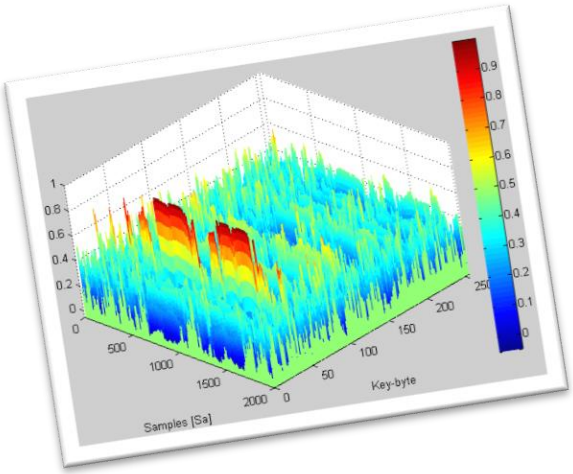
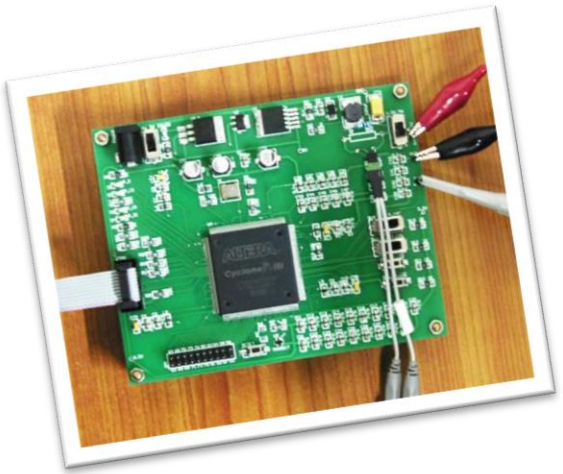


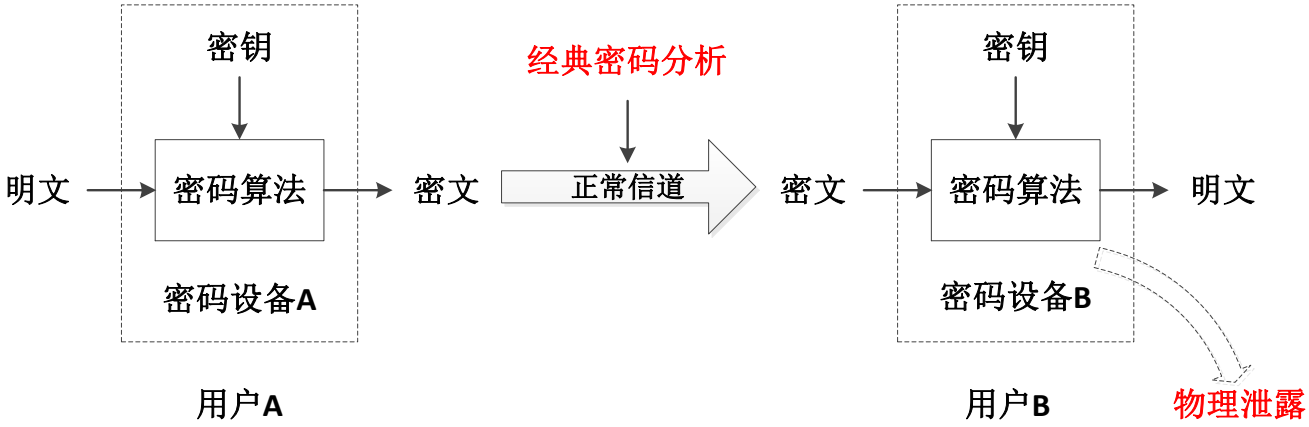


密码模块的侧信道攻击与防护实例

报告人：王安　　单位：北京理工大学计算机学院

2019年5月12日

什么是“侧信道”



火腿肠信息 → 重量

借助密码设备与外界环境存在的物理交互来恢复密钥

GM/T 0028关于非入侵式攻击的定义（附录F）

F.1 用途

本附录给出了适用于本标准的非入侵式攻击及常用的缓解方法。

F.2 非入侵式攻击

下面列出了常见的非入侵式攻击及常用的缓解方法：

能量分析：简单能量分析(SPA)和差分能量分析(DPA)。SPA 需要直接(例如，通过视觉)分析密码模块在执行密码过程中各指令的能量消耗模式。通过监视密码模块能量消耗的变化，可以发现所执行密码算法的模式和实现方法，从而获取密钥值。一阶 DPA 具有相同的目的，但是为了分析密码模块能量消耗的变化，使用了统计方法(例如，均值差、相关系数)对能量消耗进行统计分析，从而获取密钥值。二阶/高阶 DPA 针对采用防御技术的密码模块，通过分析密码模块两处/多处能量消耗的变化，使用统计方法对能量消耗进行统计分析，从而获取密钥值。现有的降低这种攻击风险的方法有：使用电容、使用内部电源、随机化密码算法或过程中的指令序列、采用双轨预充电电路来平滑能量消耗；或者采用掩码的方法，改变导致能量消耗变化的中间值。

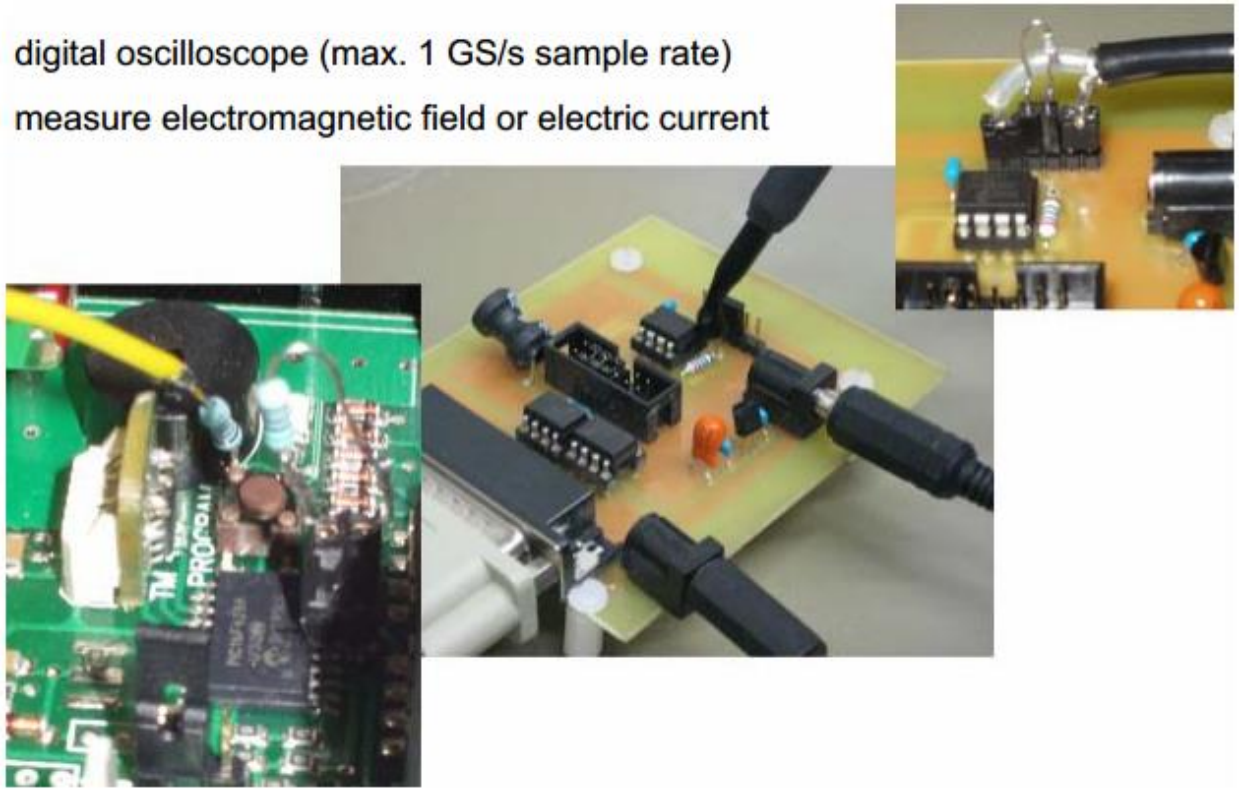
计时分析：计时分析攻击依赖于密码模块执行时间的精确测量与密码算法或过程有关的特殊数学操作之间的关系。对收集的耗时信息进行分析可以确定模块的输入和密钥之间的关系。通过对此关系的分析，从而推导密钥和关键安全参数。计时分析攻击假定攻击者具有有关密码模块的设计知识。通过控制算法或过程中各指令的运行，可以降低过程中的时间波动，这是降低这种计时攻击风险的一种方法。

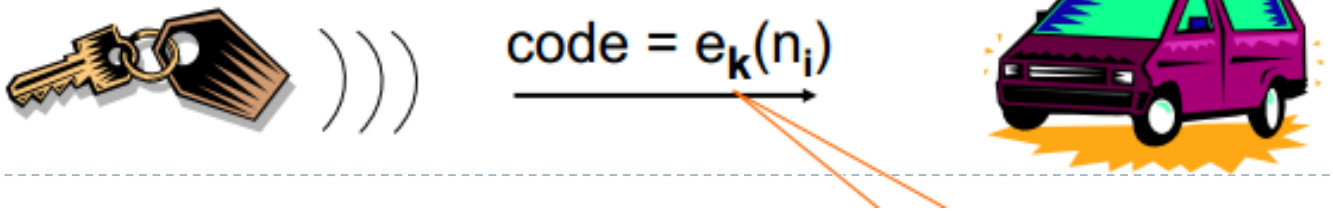
电磁泄露：电磁泄露攻击是指对正在运行的密码模块和辅助设备发出的电磁信号进行远程或外部探测和接收。通过此类攻击可以获得敲击键盘的信息，显示屏上显示的消息，以及其他形式的关键安全信息(例如，密钥信息)。通过对包括网线在内的全部组件添加屏蔽套，可以降低这种攻击的风险。屏蔽套可以减少(在某些情况下可以阻止)电磁信号的辐射。

1、十个真实侧信道攻击案例

案例1：对遥控汽车钥匙的能量攻击

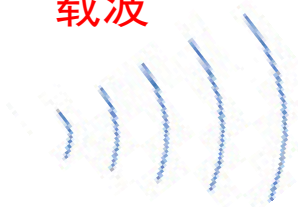
- **2008年， KeeLoq remote keyless entry systems被能量攻击技术破解 [CRYPTO 2008]**
- **目标：收发器芯片 Microchip HCS410**
- **破解方法：相关能量攻击（CPA）**





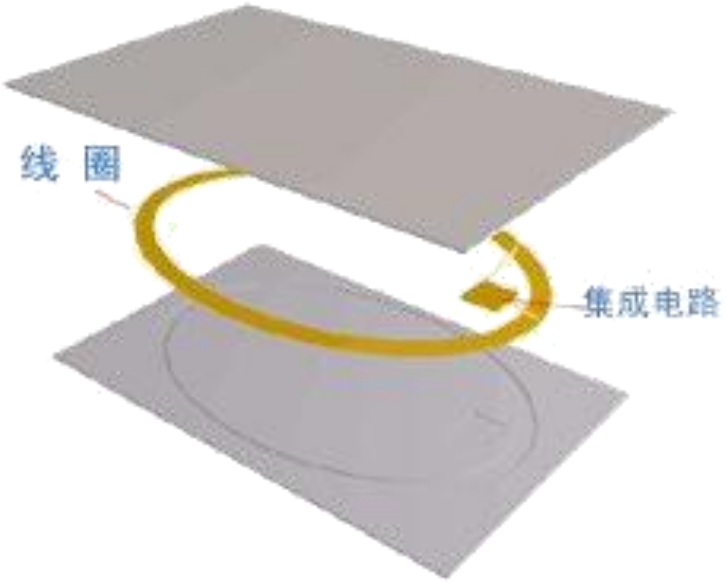
案例2：对非接触式IC卡的电磁攻击

读卡器



载波

近场探头



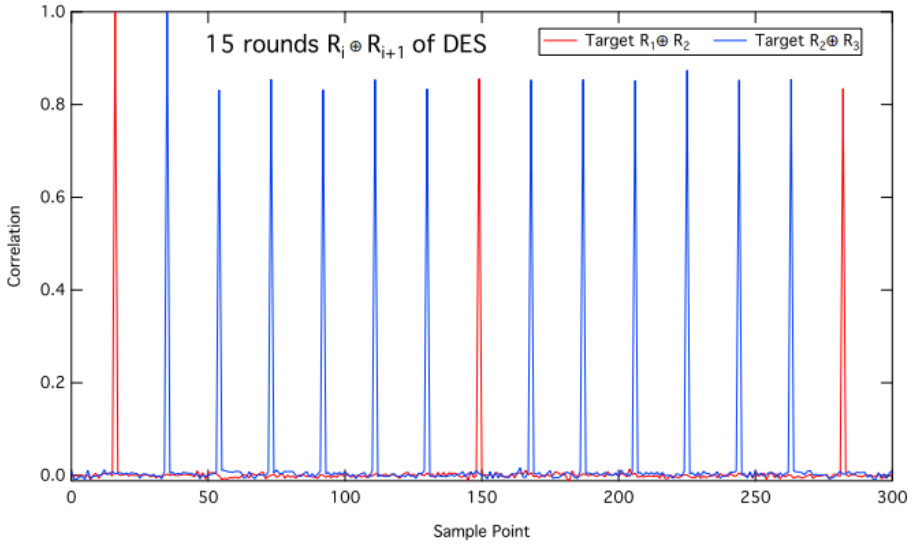
IC卡

- 2009年，Kasper等人利用侧信道攻击率先破解了RFID卡 [WISA 2009]
- 2011年，Oswald等人通过无线载波信道提取能量信息，破解了Mifare DESFire MF3ICD40非接触式智能卡 [CHES 2011]
- 破解方法：CPA、模板攻击

案例3：对“已过检”智能卡的能量攻击

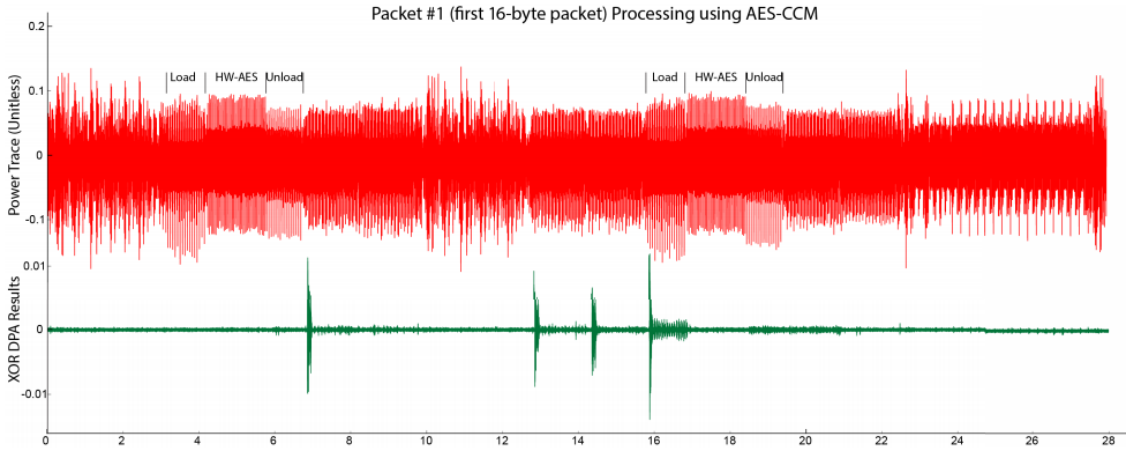
- 2017年，NXP公司破解了一款通过国际CC EAL5+安全认证的商用智能卡 [Eprint 2017, 057]
- 攻击点：DES算法的密钥生成
- 破解方法：模板攻击

	Position of round key bits 0...23 in the original key 0...55 (C–Register)																							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	8	44	29	52	42	14	28	49	1	7	16	36	2	30	22	21	38	50	51	0	31	23	15	35
2	**1**	37	22	**45**	35	7	21	**42**	51	**0**	9	**29**	52	23	**15**	**14**	**31**	**43**	**44**	50	49	**16**	8	**28**
3	**44**	23	8	**31**	21	50	7	**28**	37	**43**	52	**15**	38	9	**1**	**0**	**42**	**29**	**30**	36	35	**2**	51	**14**
4	**30**	9	51	**42**	7	36	50	**14**	23	**29**	38	**1**	49	52	**44**	**43**	**28**	**15**	**16**	22	21	**45**	37	**0**
5	**16**	52	37	**28**	50	22	36	**0**	9	**15**	49	**44**	35	38	**30**	**29**	**14**	**1**	**2**	8	7	**31**	23	**43**
6	**2**	38	23	**14**	36	8	22	**43**	52	**1**	35	**30**	21	49	**16**	**15**	**0**	**44**	**45**	51	50	**42**	9	**29**
7	**45**	49	9	**0**	22	51	8	**29**	38	**44**	21	**16**	7	35	**2**	**1**	**43**	**30**	**31**	37	36	**28**	52	**15**
8	**31**	35	52	**43**	8	37	51	**15**	49	**30**	7	**2**	50	21	**45**	**44**	**29**	**16**	**42**	23	22	**14**	38	**1**
9	49	**28**	**45**	36	**1**	**30**	**44**	8	**42**	23	**0**	52	**43**	**14**	38	37	22	9	35	**16**	**15**	7	**31**	51
10	35	**14**	**31**	22	**44**	**16**	**30**	51	**28**	9	**43**	38	**29**	**0**	49	23	8	52	21	**2**	**1**	50	**42**	37
11	21	**0**	**42**	8	**30**	**2**	**16**	37	**14**	52	**29**	49	**15**	**43**	35	9	51	38	7	**45**	**44**	36	**28**	23
12	7	**43**	**28**	51	**16**	**45**	**2**	23	**0**	38	**15**	35	**1**	**29**	21	52	37	49	50	**31**	**30**	22	**14**	9
13	50	**29**	**14**	37	**2**	**31**	**45**	9	**43**	49	**1**	21	**44**	**15**	7	38	23	35	36	**42**	**16**	8	**0**	52
14	36	**15**	**0**	23	**45**	**42**	**31**	52	**29**	35	**44**	7	**30**	**1**	50	49	9	21	22	**28**	**2**	51	**43**	38
15	22	**1**	**43**	9	**31**	**28**	**42**	38	**15**	21	**30**	50	**16**	**44**	36	35	52	7	8	**14**	**45**	37	**29**	49
16	15	51	36	2	49	21	35	31	8	14	23	43	9	37	29	28	45	0	1	7	38	30	22	42



案例4：对智能灯泡的能量攻击

- 目标：**Philips HUE智能灯**中ATMega2564RFR2芯片中的硬件AES [IEEE S&P 2017]
- 破解方法：选择明文CPA

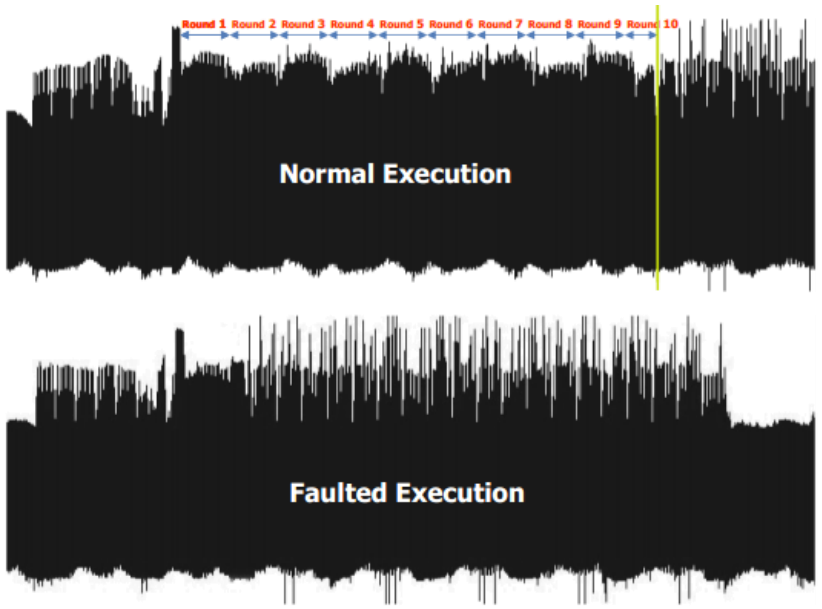


案例5：约减轮数的故障攻击 [FDTC 2005]

- 目标：Silvercard PIC16F877智能卡

- input(明文, 密钥);
- AddRoundKey();
- for (round = 1; round <= 10; round ++)
- {
  - SubByte();
  - ShiftRows();
  - if (round != 10) MixColumns();
  - AddRoundKey();
- } ← inject a fault when round = 1
- printf(密文);

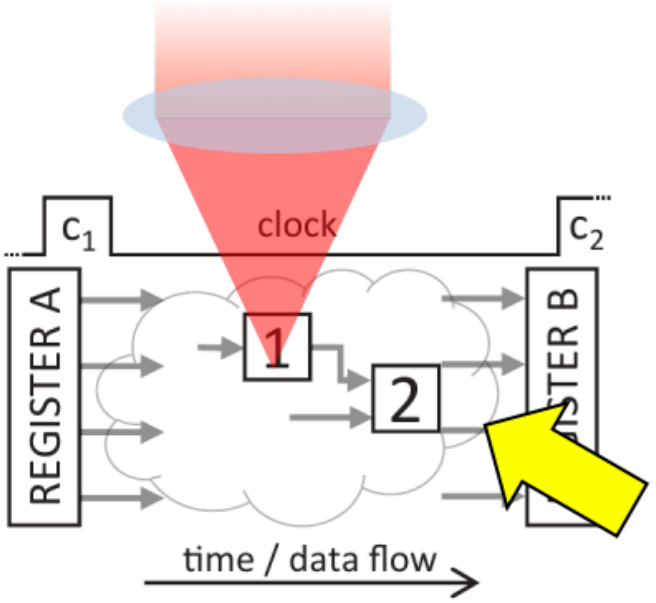
电源毛刺示例



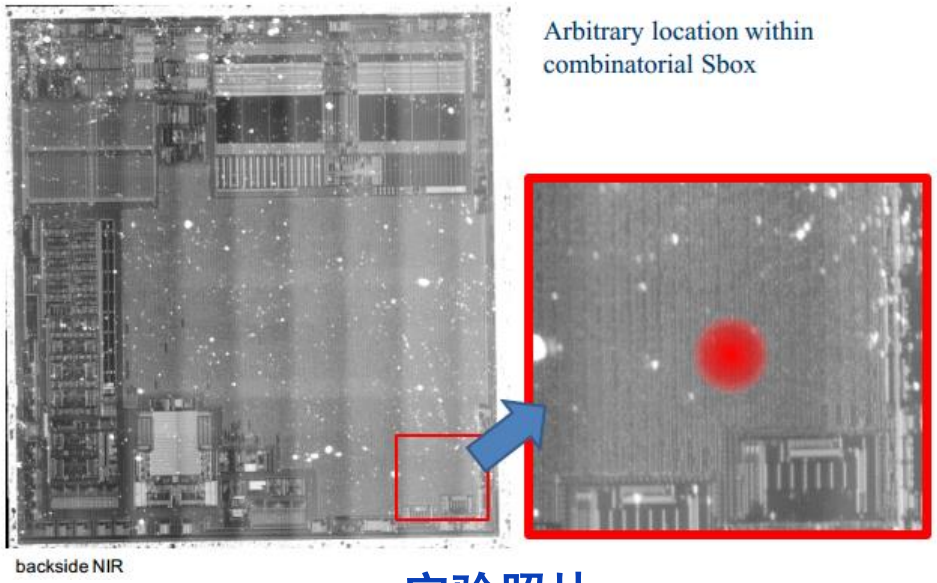
实验结果

案例6：激光故障使电路失效

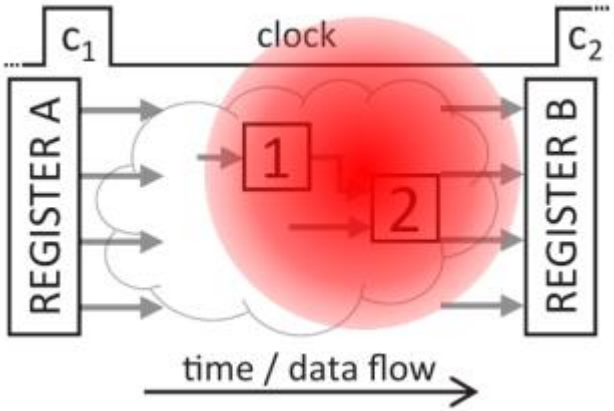
- **Large Laser Spots and Fault Sensitivity Analysis [HOST 2016]**
- **目标：ATXmega16A4U芯片中带防护的硬件AES**



激光精确注入实验示意图



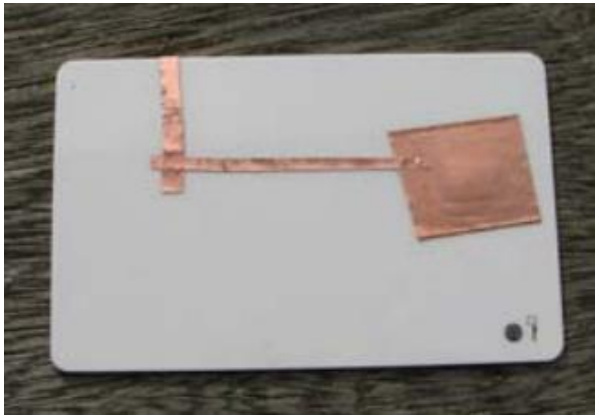
实验照片

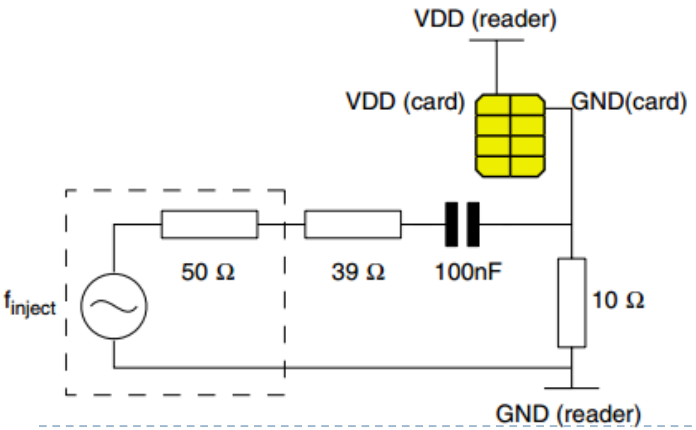


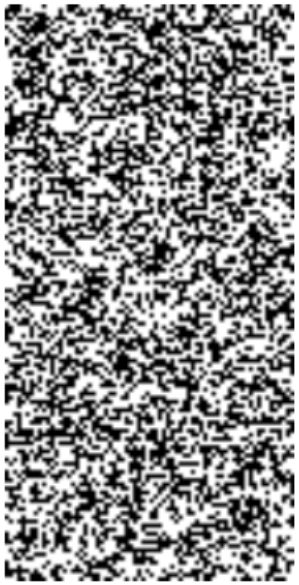
大激光点实验示意图

案例7：对真随机数发生器的频率攻击

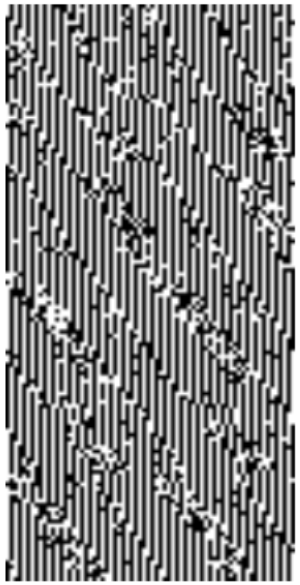
- 目标：**British High Street Bank发行的EMV银行卡中的TRNG模块 [CHES 2009]**







(a) No injection, 70 × 140 bits



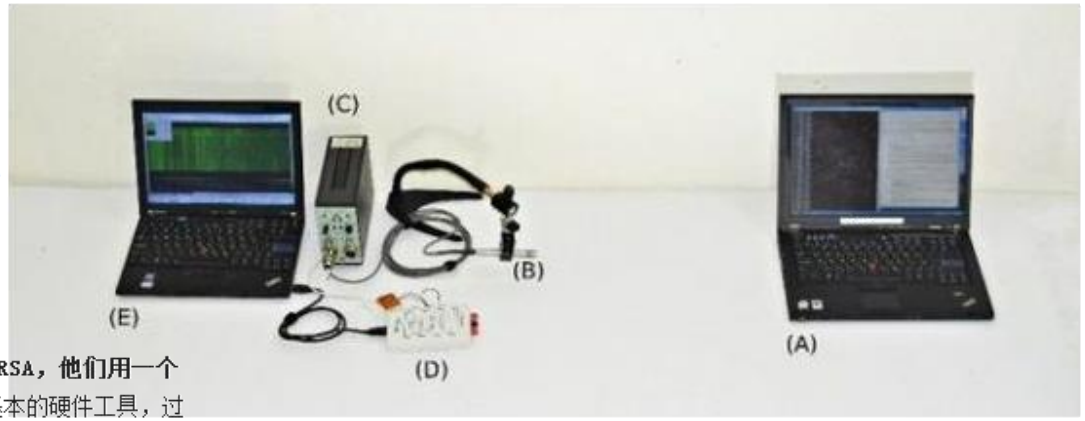
(b) 1.822880 MHz injection, 70 × 140 bits

(c) 1.929629 MHz injection, 73 × 146 bits

TRNG被电源毛刺干扰以后的统计测试结果

案例8：声音侧信道攻击

- 从声音中提取PC运行的RSA算法所消耗的能量信息 [CRYPTO 2014]



侦听CPU细微声动就可破译最严格的密钥

2013-12-19 13:54:32 来源: cnbeta网站(张越) 有0人参与 分享到

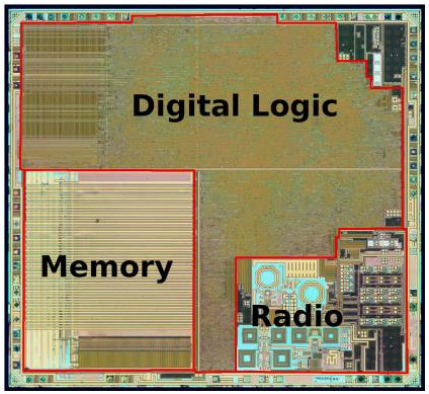
安全研究人员已经成功破译了一组最安全的加密算法4096－bit RSA，他们用一个麦克风接入到计算机侦听破解了一些被加密的数据。这次进攻利用了基本的硬件工具，过程相当简单。一般的电脑用户都是普通的大众级别，但如果是秘密特工，超级用户，或者使用其他加密类型的黑客，当破解你的加密数据时，你可能要先了解Rammstein了。

得益于一个高品质的抛物面麦克风，研究人员在距离4米的地方成功提取了解密密钥。更有趣的是，他们还设法将这种攻击实验用在了远离目标的笔记本电脑，而工具则是利用了一部30厘米外的智能手机。研究人员对不同的笔记本和台式机的进行了攻击测试，结构都获得了不同程度的成功。值得的是，相

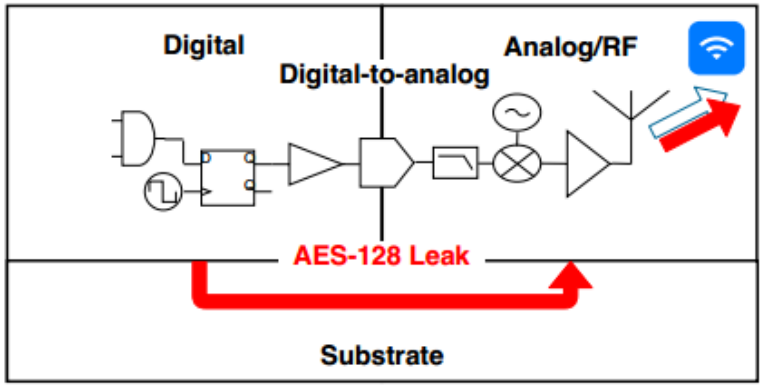
案例9：对无线电收发器实施电磁攻击

- 原理：用无线电中夹带的“AES噪声”来恢复密钥 [CCS 2018]
- 芯片：Nordic Semiconductor nRF52832
- 算法：AES（ Nordic公司tinyAES库）
- 有效距离：10米
- 信道：蓝牙

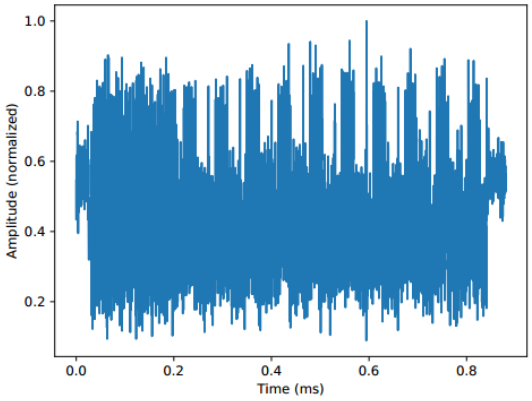
实验平台



待测芯片



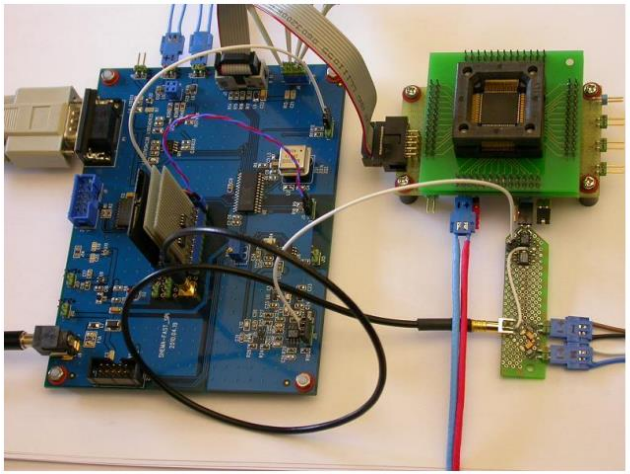
泄露原理



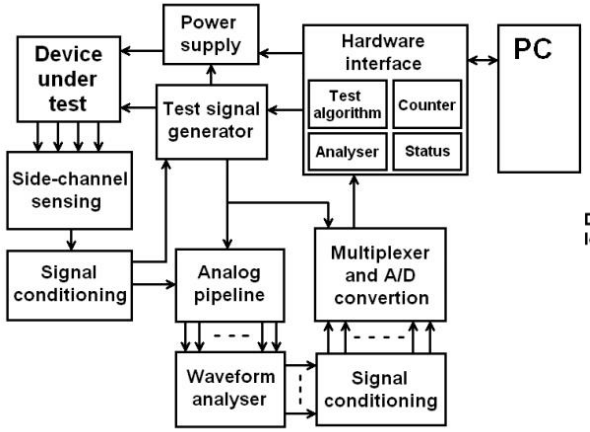
AES波形

案例10：用能量分析检测硬件木马

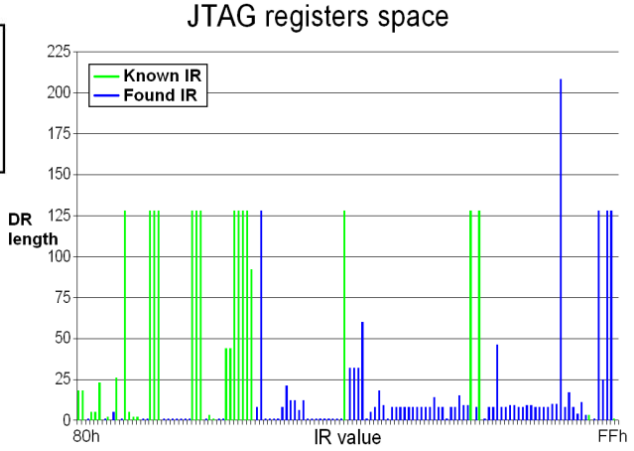
- 待测对象：军用FPGA芯片Actel ProASIC3
- 后门的用途：获得FPGA中已下载的程序
- 右图中蓝色部分为新发现的未知指令
- 后续：破解芯片内AES密钥 [CHES 2012]



平台实物图



平台原理图

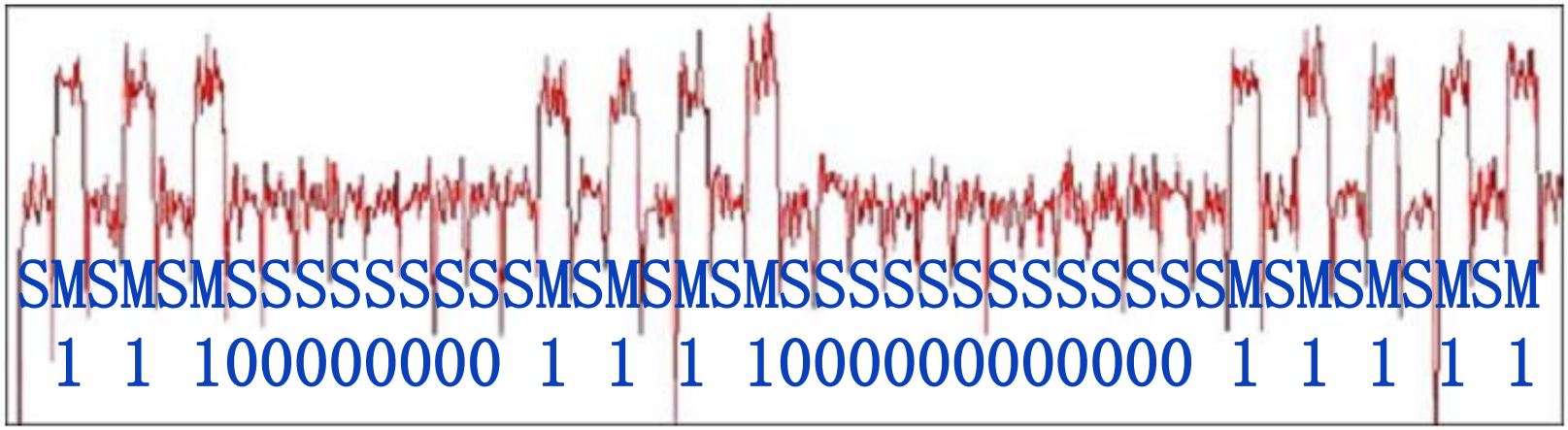


实验图

2、侧信道攻击技术

（1）简单能量分析实例（RSA算法）

输入	x，1024比特的整数$d = d_{1023} \ldots d_2 d_1 d_0$	
输出	$x^d mod\ N$	
1.	$Q = 1$	
2.	For $j = 1023$ Down to 0	
	1	$Q = Q^2$
	2	If $d_j = 1$ Then $Q = Q \times x$
3.	Return Q	



问题：RSA实现过程中如何防护该攻击？

（2）故障攻击实例

无防护实现：

SMSMSMSSSSSSSSSSMSMSMSMSSSSSSSSSSSSSSMSMSMSMSM

Dummy Operation防护：

SMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSM

Safe-Error攻击：

SMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSMSM

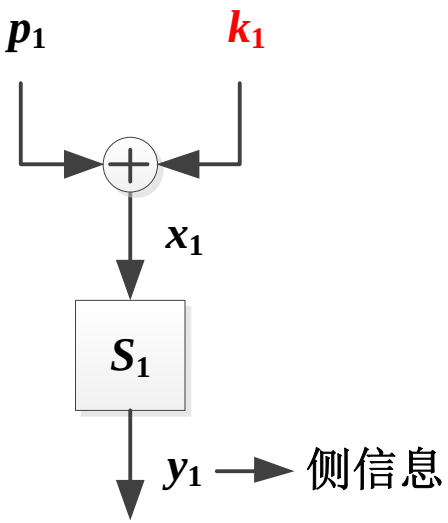
↑ 注入故障到伪操作M

↑ 注入故障到真实M

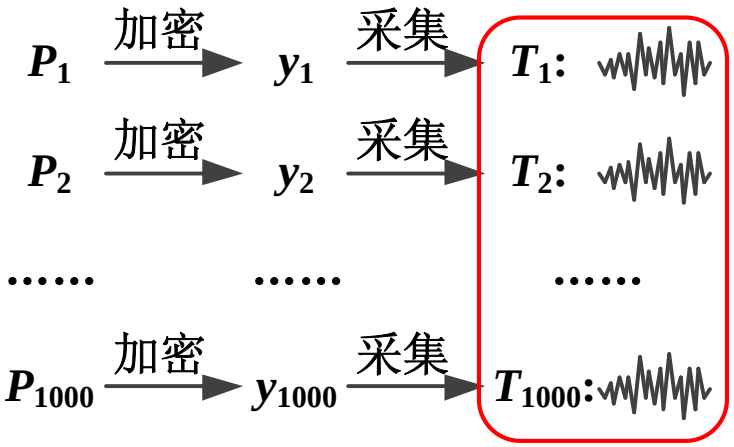
科学的RSA防护实现：

Montgomery Ladder方法

（3）相关能量分析（CPA）实例

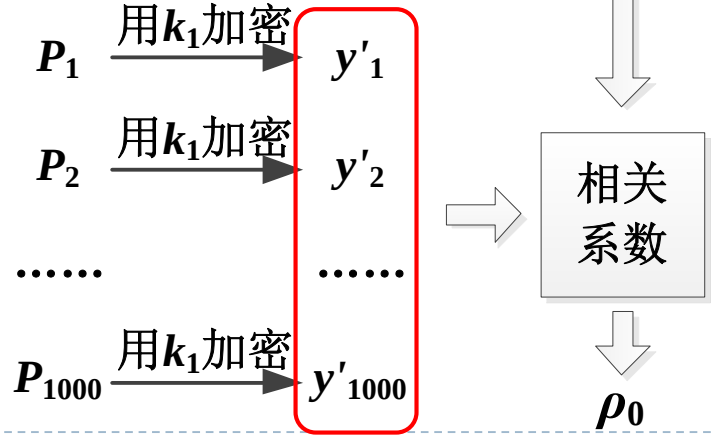


1、波形采集阶段
（单片机在线计算）



2、密钥恢复阶段
（PC离线计算）

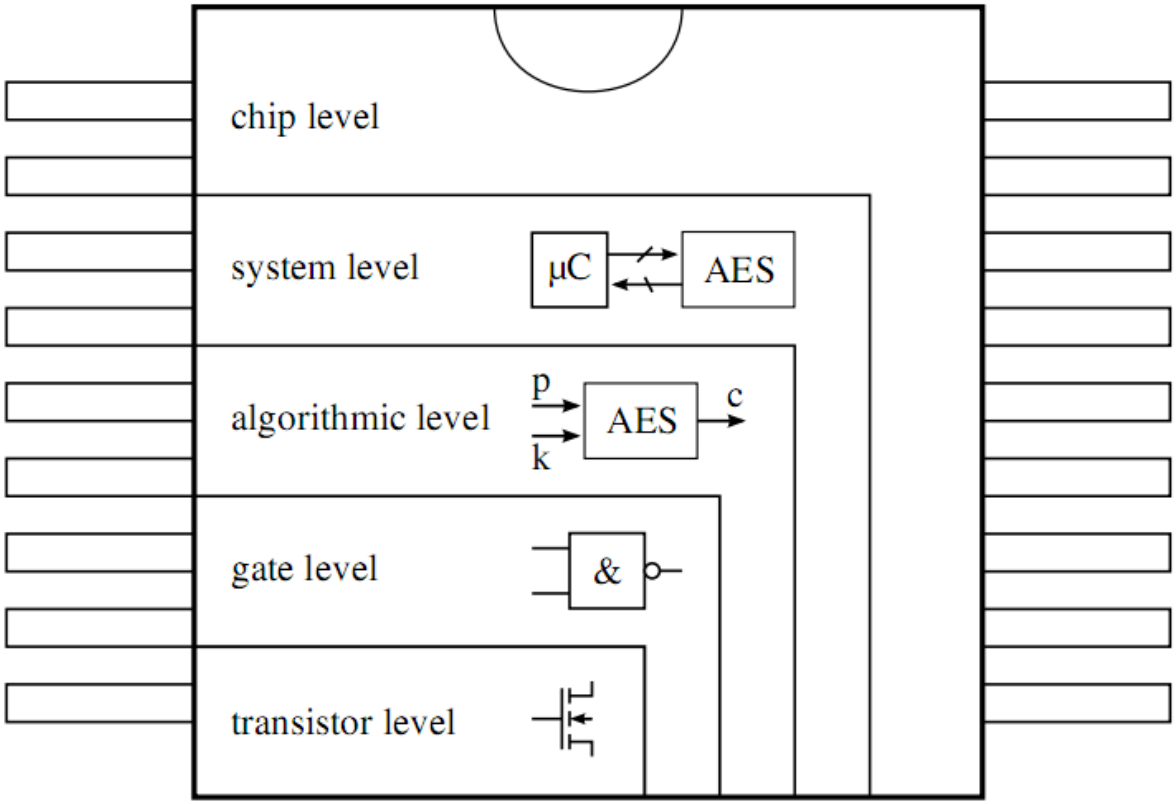
猜测 $k_1 = 0$



继续猜测 $k_1 = 1, 2, ..., 255$，得 $\rho_1, \rho_2, ..., \rho_{255}$，最大 ρ 对应正确密钥

3、密码芯片侧信道防护技术

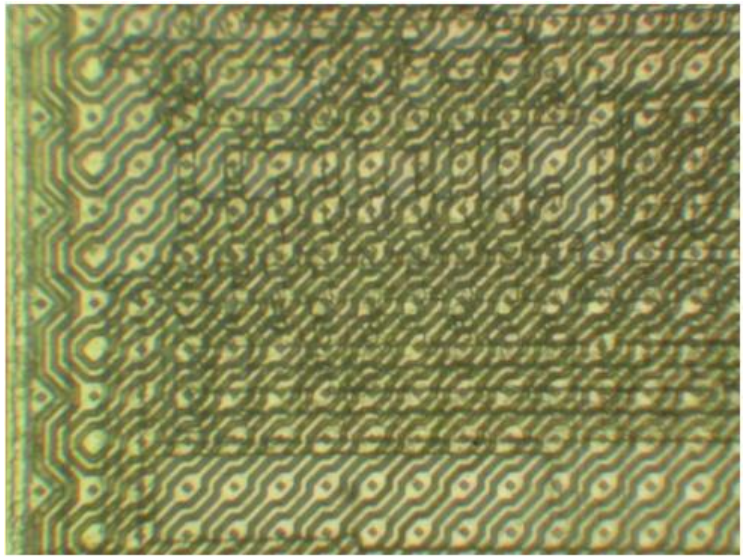
五层防御架构 [SPACE 2012]



安全性测评的重要假设：敌手知道芯片所有设计细节和源码（白盒测试）

芯片级

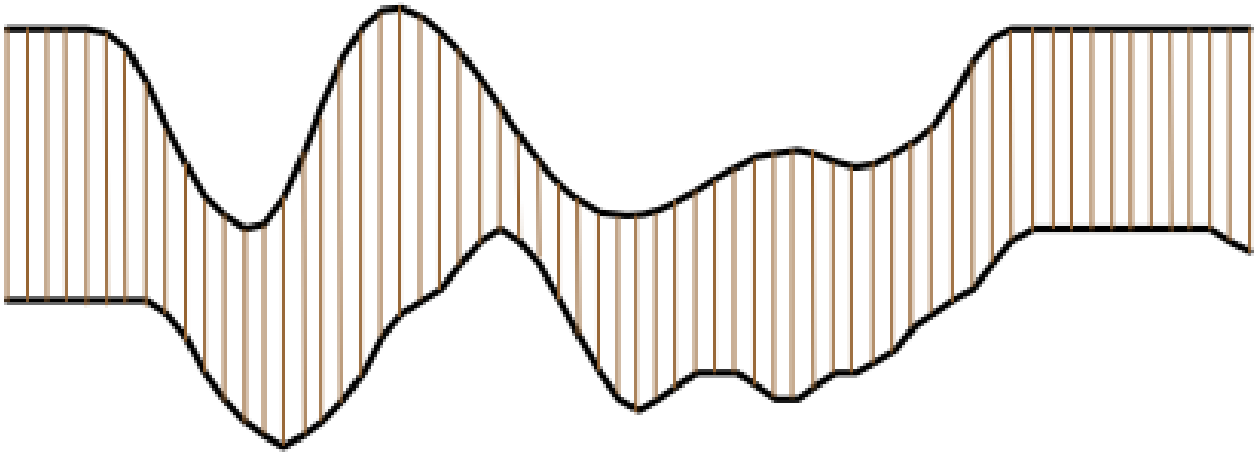
- 用传感器覆盖关键电路
  - 抗探测、FIB、激光、高频电磁波、电压毛刺、时钟毛刺等
- 在芯片的电源中引入噪声
- 用电容来缓冲电压的变化
- 随机时钟



ST16芯片表面的金属层敏感网格

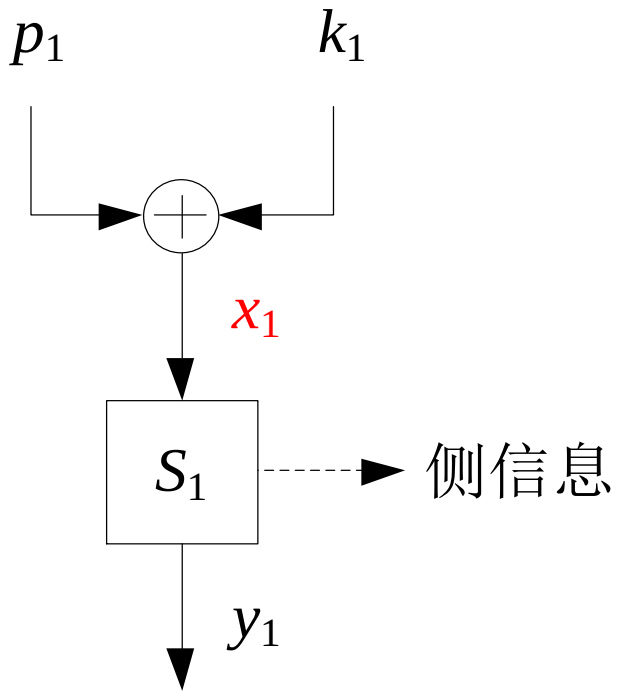
系统级

- 伪算法
- 多个密码算法同时执行
- 随机延时

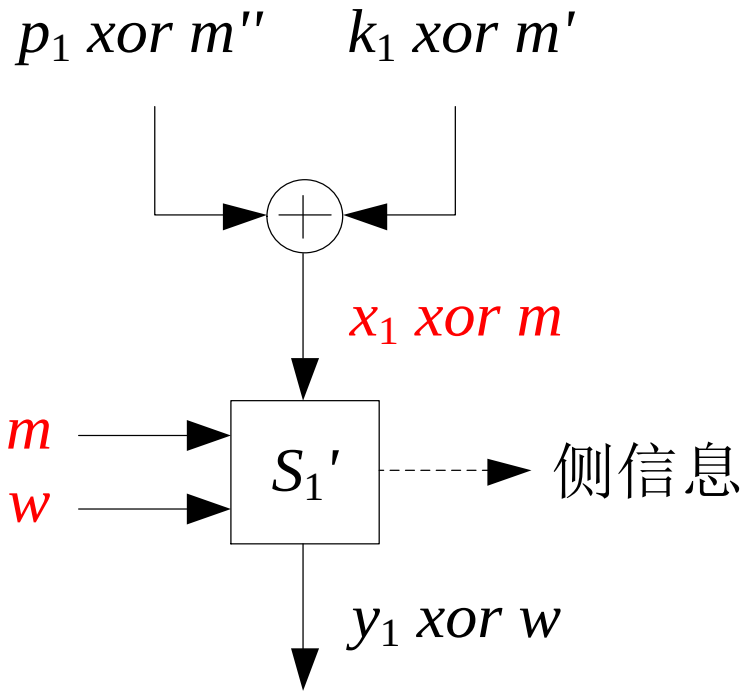


算法级

- 掩码——密码运算中间值的随机化
- 伪轮

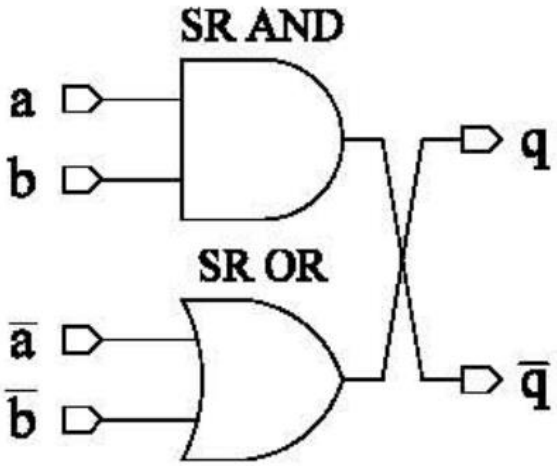


无掩码方案

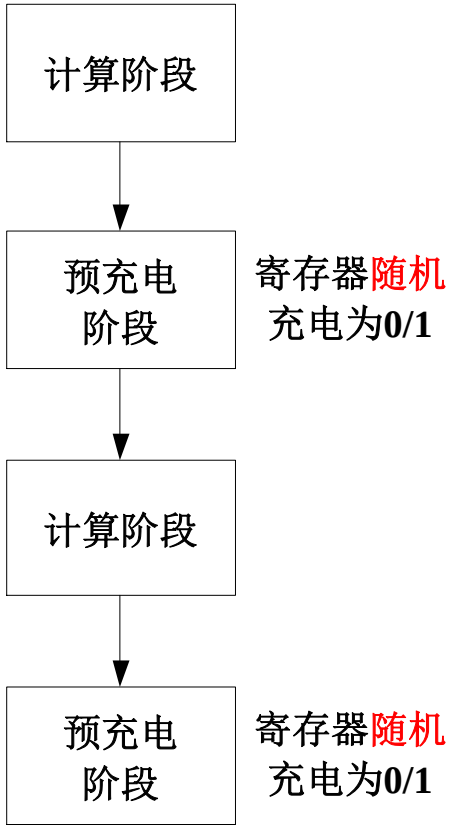


掩码防护方案

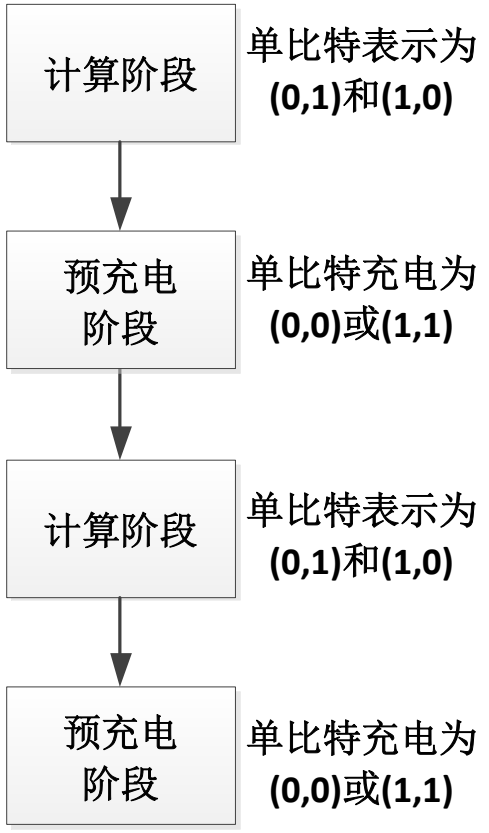
门级



双轨逻辑电路

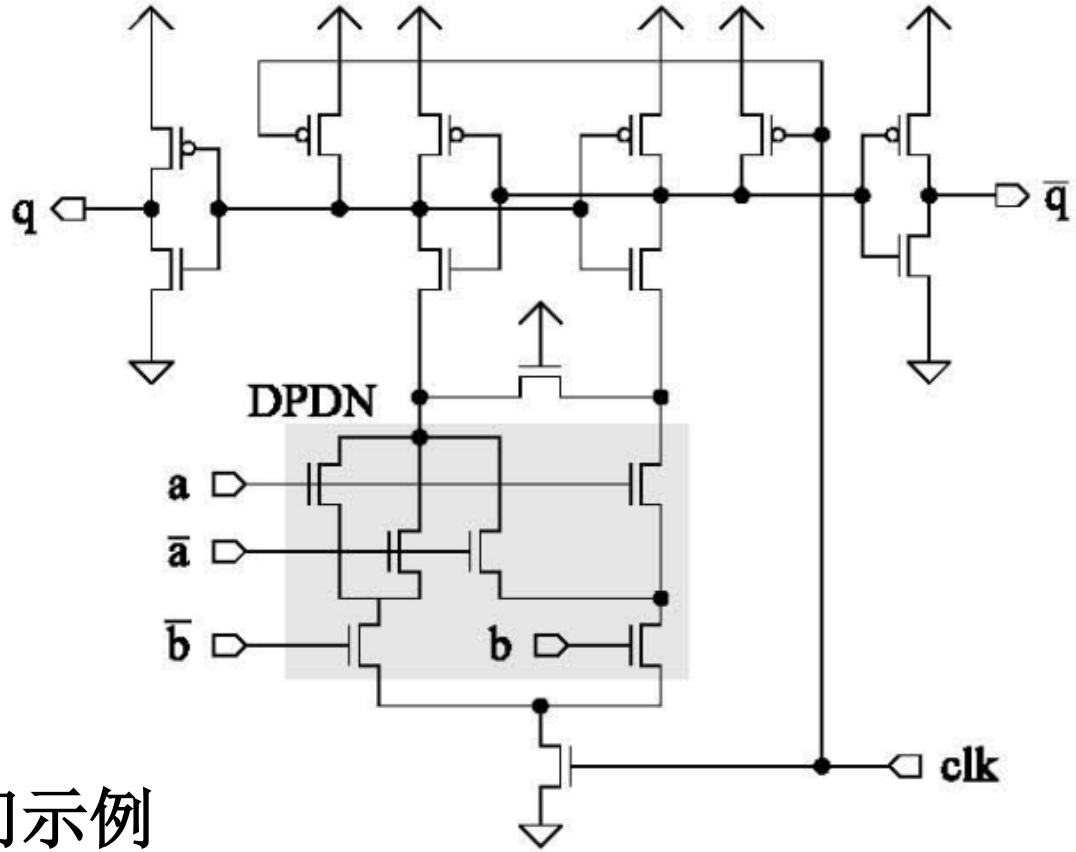


预充电逻辑



双轨预充电逻辑

晶体管级

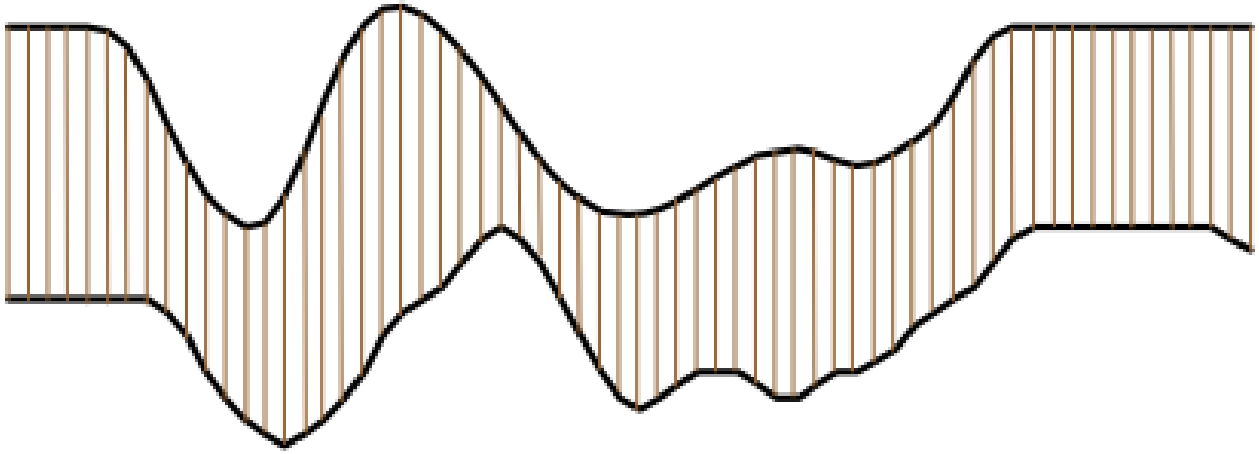


- NAND门示例
  - 当*a*、*b*至少有一个为0时，DPDN左分支导通，*q*为1
  - 当*a*=*b*=1时，DPDN右分支导通，*q*为0

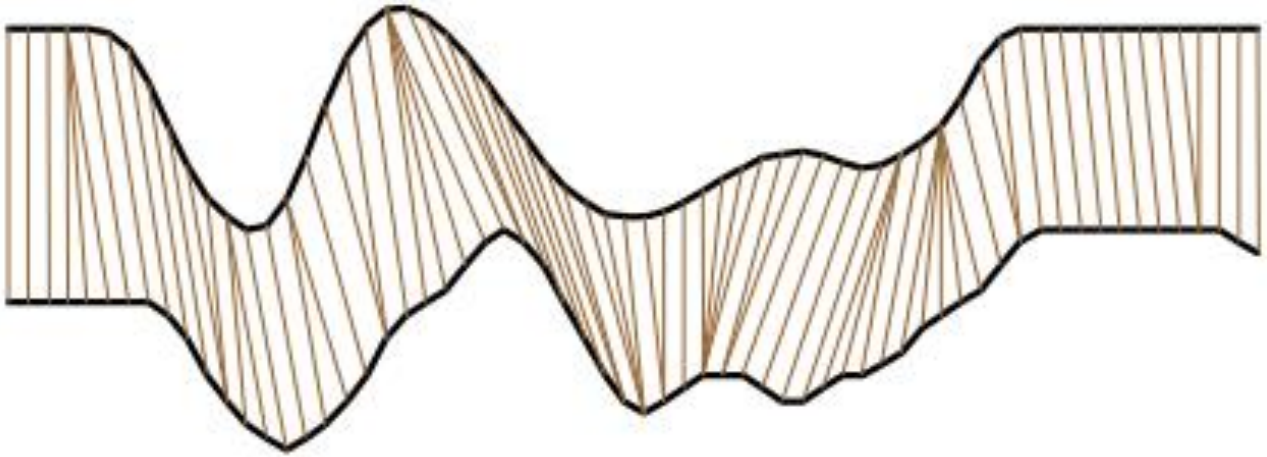
4、针对防护对策的高级攻击技术

攻击随机延时对策——弹性对齐算法

- 普通对齐

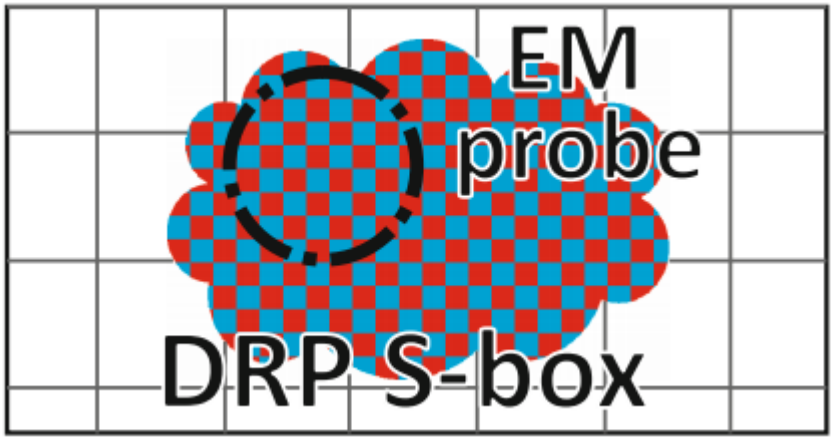


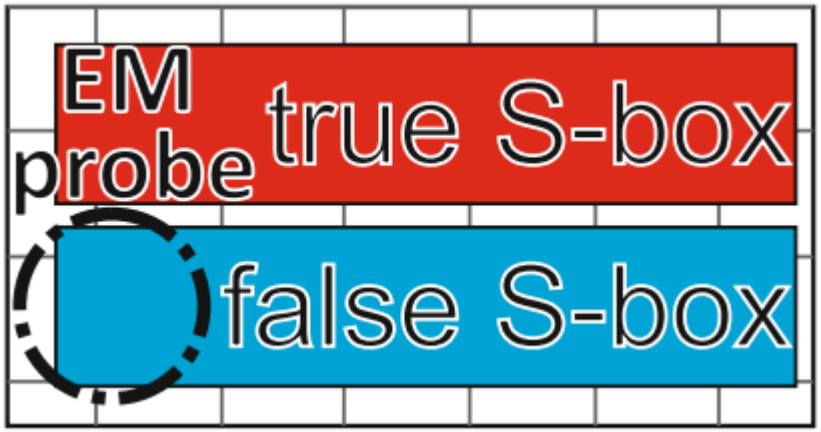
- 弹性对齐



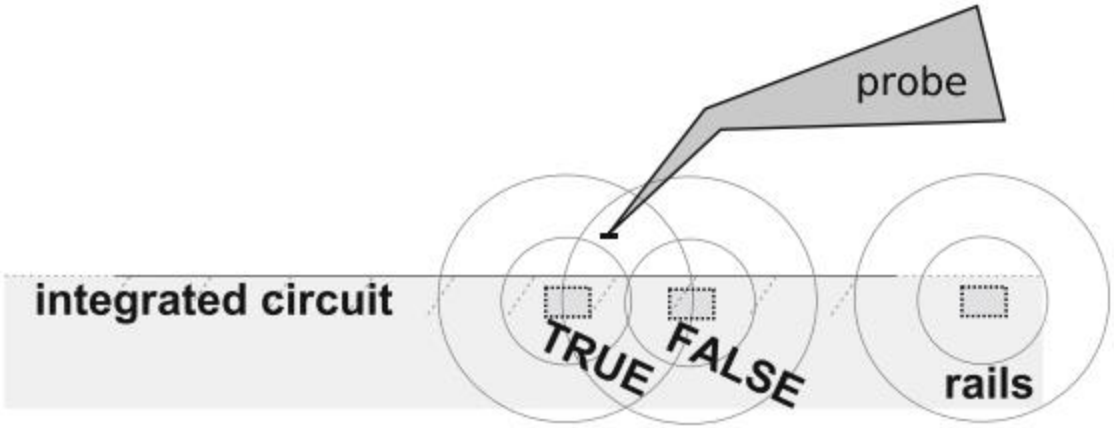
另：海量波形进行统计，仍可以攻破大多数防护对策

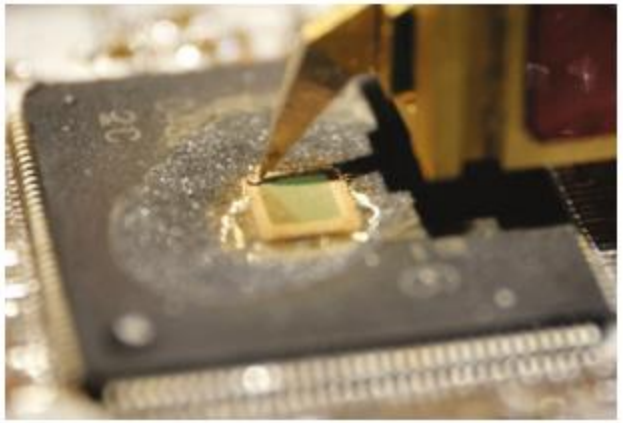
攻击双轨逻辑对策——电磁攻击





针对双轨逻辑的电磁攻击原理

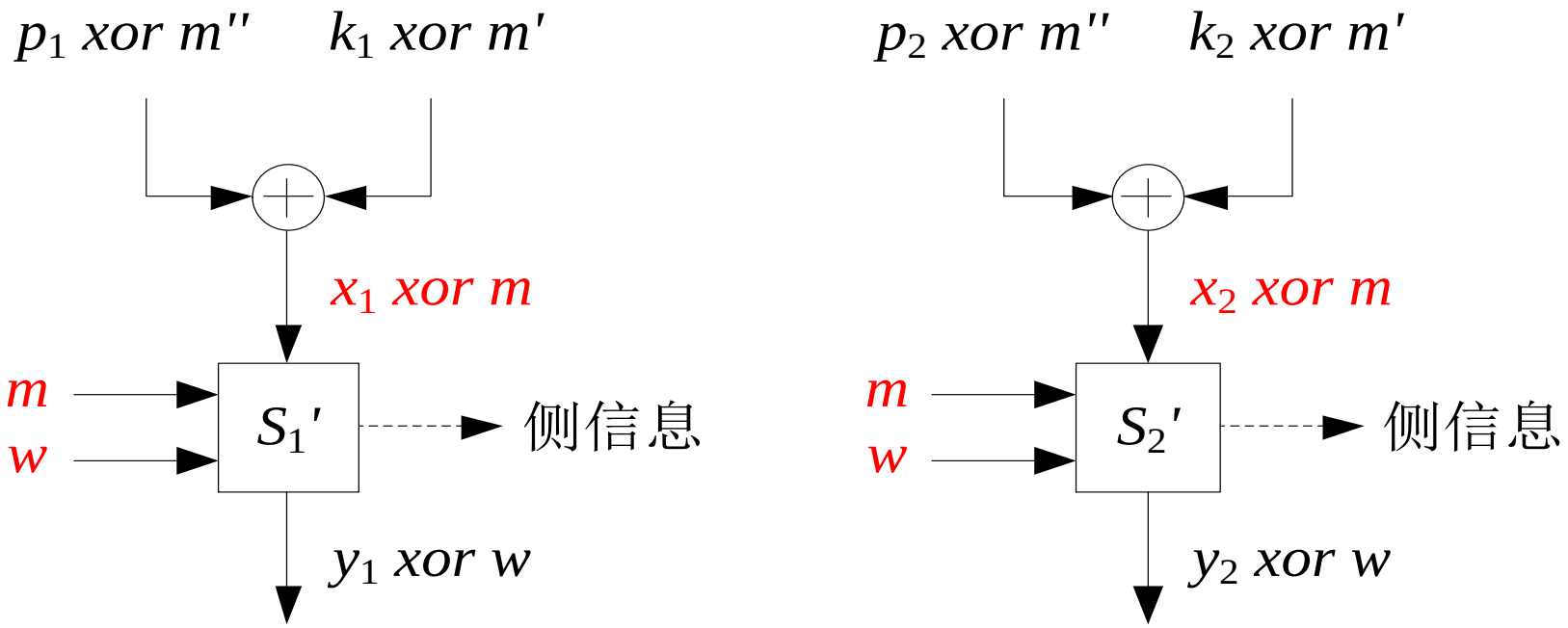




探头放置空间位置示意图

二阶CPA攻击 [CT-RSA 2006]

- 思路：猜k_1和k_2，用 $|T_1\text{-}T_2|$ 与 $|\mathrm{HW}(x_1 \oplus x_2)|$ 计算相关系数



5、总结

总结

- 洛卡尔物质交换定律：犯罪行为人只要实施犯罪行为，必然会在犯罪现场直接或间接地作用于被侵害客体及其周围环境，会自觉或不自觉地遗留下痕迹
- 密钥0和1的不同，也必然会显现出不同特征，我们需要做的，是把这些特征淹没在足够的噪声中

vs

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

欢迎各位专家老师批评指正！

报告人：王安
邮箱：wanganl@sina.com
QQ：1134277
电话：13466788373
地址：北京市海淀区中关村南大街5号北京理工大学中心教学楼838室

GM/T 0028关于非入侵式攻击的阐述

7.8 非入侵式安全

非入侵式攻击是指没有通过物理方式修改或入侵模块就可以获取模块关键安全参数相关信息，从而破坏模块安全性的一种攻击手段。模块可以实现各种技术来缓解这些类型的攻击。对于本标准提出的每一个安全功能，其对应的非入侵式攻击的缓解测试指标应符合国家相关部门的有关要求。

如果由密码模块实现、用于保护模块关键安全参数的非入侵式攻击的缓解技术不在附录 F 中，则这些技术“应当[08.01]”满足 7.12 中规定的要求。

如果由密码模块实现、用于保护模块关键安全参数的非入侵式攻击的缓解技术在附录 F 中，则这些技术“应当[08.02]”满足下列要求。

模块文档“应当[08.03]”按照 A.2.8 中规定的要求编写。

a) 安全一级和二级：

对于安全一级和二级，文档“应当[08.04]”阐明用于保护模块关键安全参数免受附录 F 中的所有非入侵式攻击的缓解技术。如果有相应措施，文档“应当[08.05]”包括可以证明每个缓解技术有效性的证据。

b) 安全三级：

对于安全三级，除了安全一级和二级的要求，密码模块“应当[08.06]”实现用于保护模块关键安全参数免受附录 F 中的所有非入侵式攻击的缓解技术，文档“应当[08.07]”包括可以证明每个缓解技术有效性的证据，并提供测试方法。

c) 安全四级：

对于安全四级，除了安全一级、二级和三级的要求，密码模块“应当[08.08]”接受测试以满足国家相关部门规定的非入侵式攻击缓解测试指标的要求。

GM/T 0028关于非入侵式攻击的阐述

7.12 对其他攻击的缓解

密码模块可能还容易受到一些在本标准内其他条款未定义的攻击，模块对攻击的敏感性取决于模块的类型、实现以及实现环境。恶意环境(例如，攻击者可以是模块的授权操作员)中的密码模块可特别关注这些攻击。这些攻击通常依赖从模块物理外部获得的一些信息进行分析，以确定关于密码模块中关键安全参数的某些信息。

模块文档“应当[12.01]”按照 A.2.12 中规定的要求编写。

a) 安全一级、二级和三级：

如果将密码模块设计为可缓解一种或多种在本标准中未定义的特定攻击，那么模块的相关文档“应当[12.02]”列举出模块能够缓解的攻击。当制定出要求以及相关测试后，将对用于缓解攻击的安全机制进行验证，测试其是否存在且是否起作用。

b) 安全四级：

除了安全一级、二级和三级的安全要求，安全四级的密码模块还“应当[12.03]”满足下列安全要求：

——如果声明了能够缓解本标准未定义的特定攻击，则文档“应当[12.04]”详细说明缓解攻击的方法以及测试该缓解技术有效性的方法。