概念：

1.侧信道攻击——是一种利用计算机不经意间释放出的信息信号（如功耗,电磁辐射，电脑硬件运行声）来进行破译的攻击模式：例如，黑客可以通过计算机显示屏或硬盘驱动器所产生的电磁辐射，来读取你所显示的画面和磁盘内的文件信息；或是，通过计算机组件在执行某些程序时需要消耗不同的电量，来监控你的电脑；亦或是，仅通过键盘的敲击声就能知道你的账号和密码。

2.侧信道分析又称侧信道攻击，是一种针对密码实现（包括密码芯片、密码模块、密码系统等）进行攻击从而最终分析出密钥的方法。随着集成电路技术的发展，密码算法以硬件电路的实现方式出现在密码设备中。在实际应用中，这些硬件设备会泄漏出能量、电磁等多种类型的物理信息，称为侧信息。侧信道分析技术利用这些信息，能够直接或间接获取密码算法运算过程中的中间值信息，进而可以分段恢复较长的密钥。

3.侧信道分析的方法（？）：

（1）唯密文攻击：通过一段或多段密文来推测密钥，这种方法很低效。

（2）已知密文攻击：有一些通过同一密钥加密的密文及其明文，通过这些推断密钥

（3）选择明文攻击：攻击者可以随意选择明文进行加密得到密文，由此恢复密钥

（4）选择密文攻击：攻击者可以随意选择密文进行解密，由此恢复密钥

4.物理攻击是指，攻击者通过物理手段（一般会借助相关的仪器仪表等）对芯片的物理特征进行窥探（如电压、时钟、能量辐射等），以及破坏行为（如对芯片的剖片、物理克隆等），从而达到获取内部程序或数据的目的。

基于芯片被攻击后是否被破坏，物理攻击可分为三种类型：侵入式攻击、半侵入式攻击和非侵入式攻击。（众所周知，侧信道攻击（SCA: Side-channel attack）就属于非侵入式攻击。时序攻击和功耗攻击是典型的侧信道攻击方法。）

设计：

1.功能包括：泄露信息显示（功耗、电磁）、侧信道分析（泄露信息分析攻击，至少4个）、脚本控制、抗物理攻击设计（按钮）

2.泄露信息显示：给定两个方框页面用于显示功耗和电磁曲线。

3.泄露信息分析（SPA、DPA、CPA等侧信道攻击手段）：侧信道分析界面暂时模仿编程IDE得交互逻辑来做（做不到），需要一个输出页面输出分析后的结果。

4. 差分传输管预充电逻辑（CP2L逻辑）：作用：使功耗曲线恒定（抗物理攻击）





