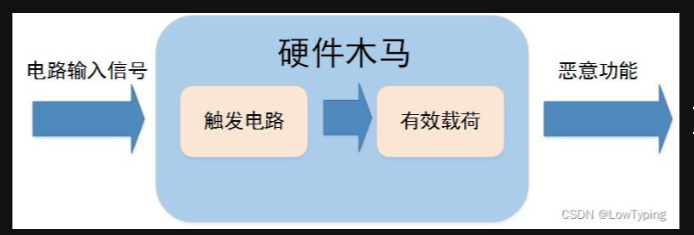
概念：

1.硬件木马结构特征：硬件木马通常包括两个基本结构，即触发逻辑和有效载荷，如下图所示。触发逻辑的功能是监听预设的触发信号，在接收到指定信号或满足特殊条件时激活植入的有效载荷，触发信号多种多样，如组合逻辑、数字逻辑等数字信号，温度、电压等模拟信号；常见的触发逻辑结构有简单组合逻辑触发、伪随机数生成器、时序性结构及状态机等。有效载荷是用来实现硬件木马功能的主体电路，当触发逻辑满足条件时，有效载荷部分使能，并按照木马设计者设定的方向运转，实现原本电路所不具备的恶意功能，如信息泄露、参数修改、功能改变等。



2.硬件木马检测方法：硬件木马具有很大的潜在威胁，及时准确的检测其恶意行为对用户来说十分重要，随着技术的革新，检测方法也在不断发展。传统的硬件木马检测技术包括侧信道分析法、逻辑测试检测法（通过测试阶段触发木马，得以确定木马）和逆向工程检测法，大数据和人工智能技术的发展使得基于机器学习的硬件木马检测技术也逐渐成熟。

3.逆向工程检测方法：逆向工程法指的是通过对样本芯片进行解剖获得具体的版图信息，从而分析出电路的逻辑结构，将得到电路设计结构与原始设计文件对比，直观判断是否有木马植入。该方法是最直接、最典型的检测方法，且已经形成了较为完善的体系，不仅能够找出植入硬件木马的芯片，还可以检测出硬件木马的具体位置、构造以及木马对芯片造成的影响等。但这种方法也有明显缺点：一是成本高且耗时长，必须完整逆向芯片全部功能才能分析出硬件木马；二是具有破坏性，仅对抽样芯片的检测不能完全说明问题，对于整组芯片还需要进行额外测试。

页面设计：

1.功能包括：侧信道分析检测、逆向工程检测（版图检测）、逻辑测试检测