旁路攻击SCA及防御

密码攻击

- 攻击方法

> 数学攻击
>
> 实体攻击
>
> - 需要昂贵的高端实验室设备和专门的探测技术
>   - 昂贵是相对的，有专门提供这种服务的话就较偏移
>
> 实现攻击
>
> - 种类
>
>   - 主动式攻击(失效分析攻击)
>
>   - 是一种侵入式攻击，通过**引入故意错误**如数据都懂、电源或时钟突变来影响加密电路的正常运算过程
>   - 常见干扰方式
>   - 时钟信号扰动
>   - 最容易和有效的干扰方式
>   - 电源供应短暂扰动
>   - 外部电磁场短暂扰动
>   - ……
>   - 干扰攻击的目的
>   - 逃避安全检查
>   - 采集信息
>   - 使cpu执行非法指令，泄露安全信息
>   - 减短程序循环的次数
>   - 例如密码运算的轮加密
>
>   - 被动式攻击(旁路攻击)
>
>   - 基于统计理论的物理攻击方法
>
>   - 必要条件
>
>   - 足够多的样本数据
>   - 各密钥相关状态的准确采样值
>
>   - 分类
>
>   - 时间攻击
>   - 故障攻击
>   - 功耗攻击
>   - 电磁攻击
>   - 声音攻击

        - 可见光攻击
        - 组合分析攻击

        > 能量攻击和电磁攻击最为强大和高效

    - 相对廉价且有效
    - 与传统的数学分析方法相比，具有较小的密钥搜索空间

工业控制系统信息安全

- 基本概念
    - 工业控制系统ICS是综合集成了计算机、网络、现代通信、微电子以及自动化技术，是对多种控制系统的总称，包括

        - PLC
        - SCADA
        - DCS