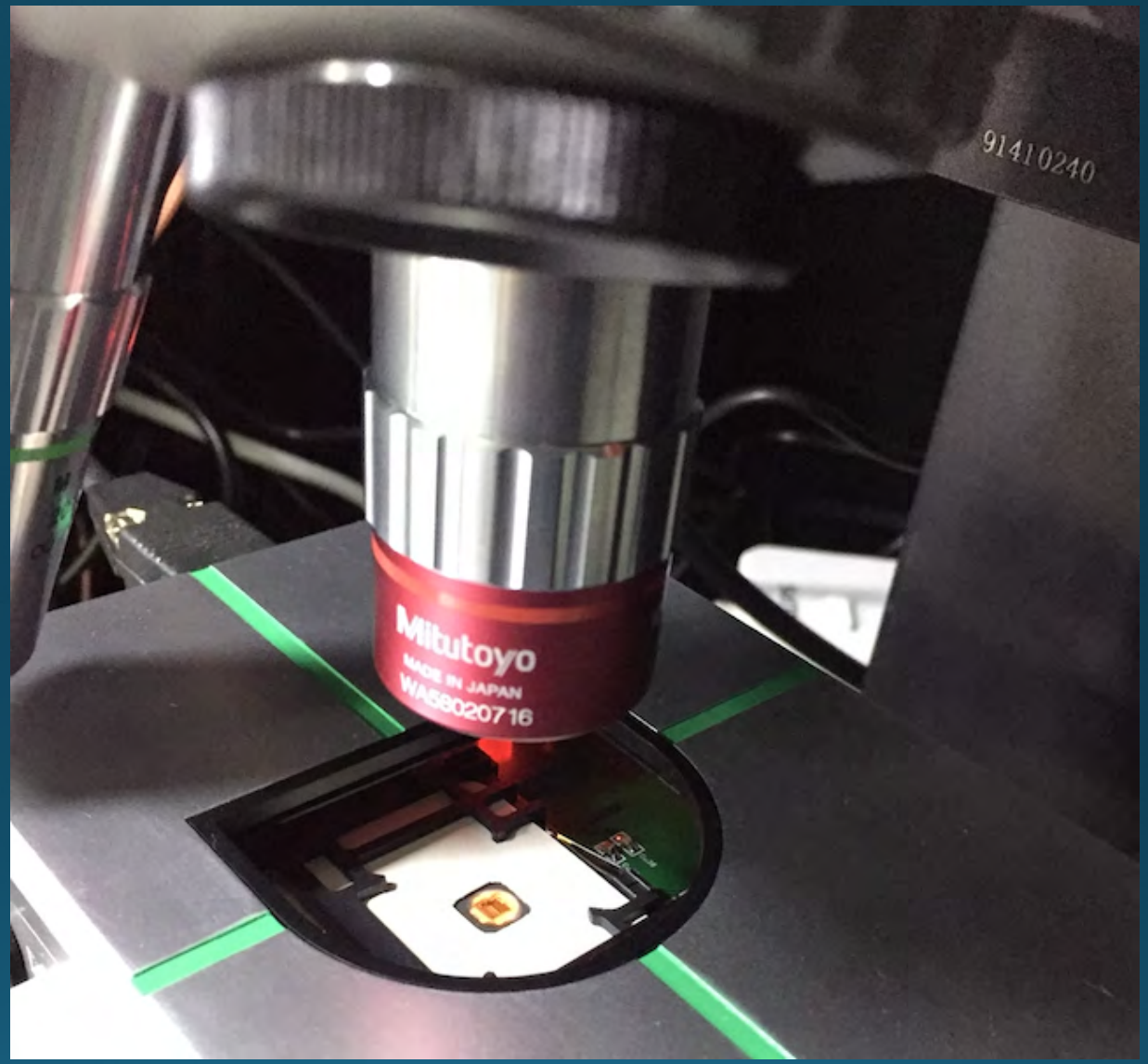
设备简介



智慧云测

产品列表

芯片安全攻击设备

- 侧信道测试平台
- 单点激光测试平台
- 多点激光测试平台
- 智能毛刺测试平台
- 传感器功能验证
- 电磁操纵测试平台
- 存储器加解密测试软件

嵌入式软件安全攻击设备

- 嵌入式软件攻击平台
- 卡片入网测试平台
- 断电测试平台
- 随机数发生器测试软件
- TEE测试平台
- 防火墙测试平台
- Cache攻击测试平台

设备优势

国产优势

- 符合国家信息安全大战略
- 符合国内金融、PBOC、EMVCo、CC等标准规范
- 国内首家全系列商用安全检测工具
- 设备具完全自主知识产权

技术优势

- 团队拥有超过6年安全领域行业经验
- 多人获得人民银行科技进步特等奖
- 参与行业内多个标准编写
- 领域内发表论文10余篇；发明专利10余项

支持优势

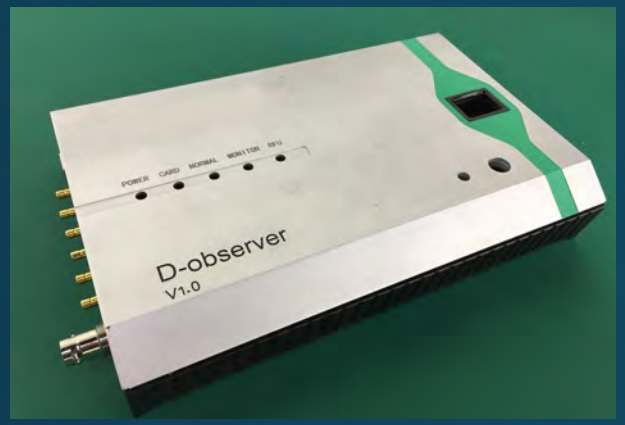
- 国内本地化技术支持团队
- 承诺7*12小时电话技术支持
- 承诺96小时解决技术问题
- 按需定制升级设备
- 兼容国际主流检测设备

平台优势

- 合作运营模式灵活
- 平台化、操作维护简单

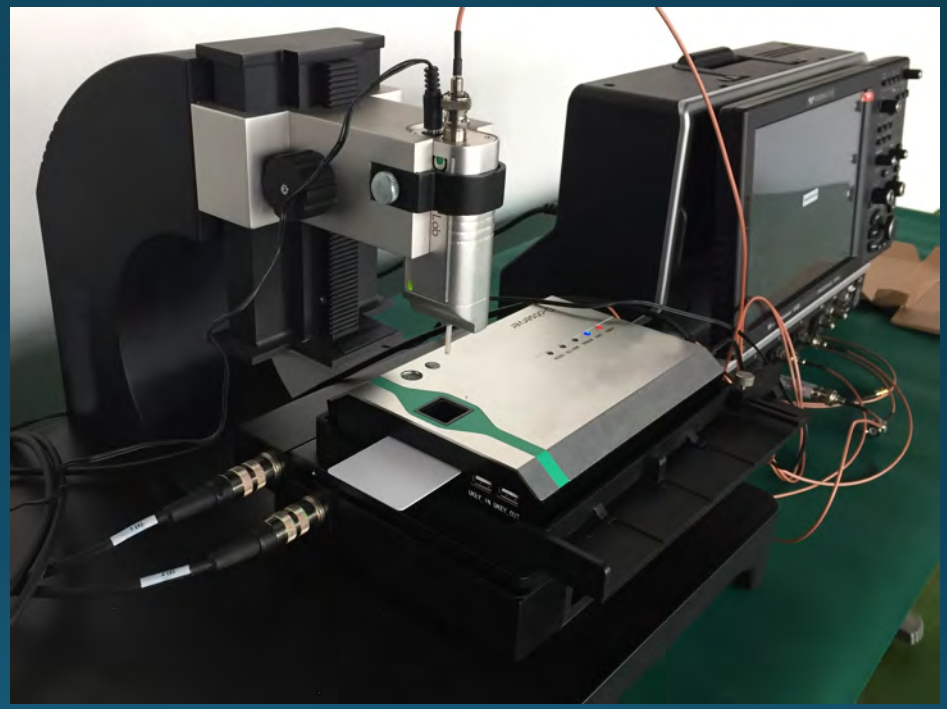
一、侧信道设备

a，部分硬件外观图



功耗采集模块

电磁探头



电磁采集+功耗采集平台

一、侧信道设备

c，侧信道设备组件

序号	软件组件	用途说明
1	侧信道软件平台	对已采集的曲线进行分析处理，获取密钥信息
2	国密算法包	增加对国密算法SM2，SM4的支持

序号	硬件组件	用途说明
1	电流采集模块	对被测物的电流能量进行采集，适用于所有电子类被测物
2	功耗采集模块	对被测IC卡片进行功耗能量采集，支持传统、改进、电流方式采集
3	电磁采集模块	对被测物的电磁辐射能量进行采集，适用于所有电子类被测物
4	测试工作站	运行侧信道软件平台，对采集曲线进行分析处理
5	高级示波器	高精度采集能量曲线，观察信号波形，方便定位扫描位置

一、侧信道设备

f, 攻击流程

Step 1 采集部分

- 分析被测对象，选择最优采集方式
- 编写采集脚本，循环运行

Step 2 曲线处理

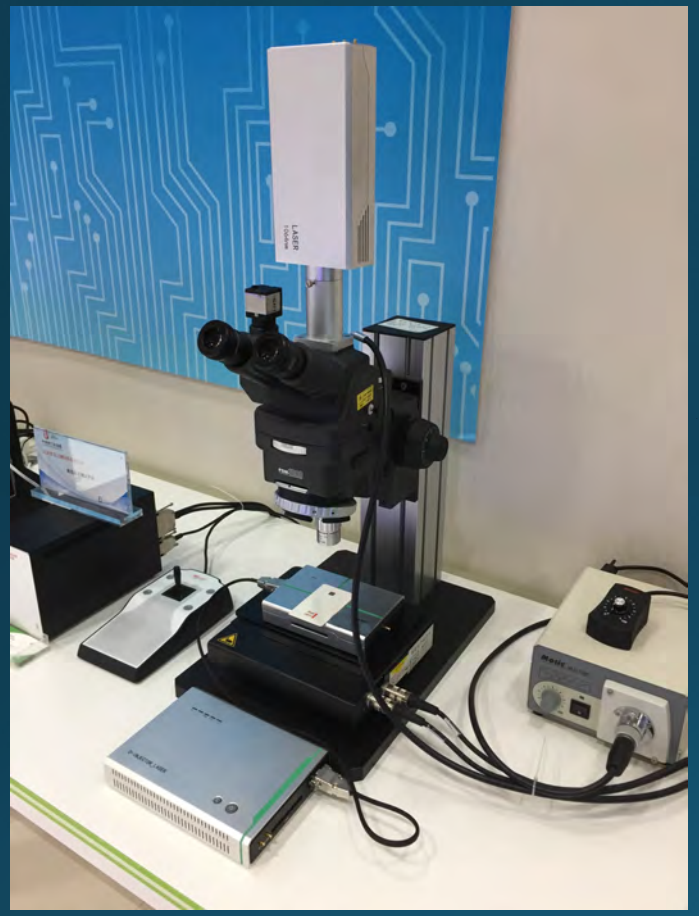
- 滤波处理
- 对齐处理
- 压缩处理
- 相关性分析
- 泄露特性分析

Step 3 密钥分析

- SPA
- DPA
- EMA
- 模板攻击

二、错误注入设备

a，部分设备外观



单点激光注入
工作台

多点激光注入
工作台

电压毛刺注入模块

电磁注入模块

二、错误注入设备

b, 关键特性

激光波长注入攻击

- 1064nm（近红外）
- 808nm（红）
- 455nm（蓝）

精确的电压毛刺攻击

- 电源毛刺产生最小宽度4ns

电磁注入攻击

- 电磁最小脉冲时间宽度10ns

交互更精准

- 支持和被测芯片进行单指令交互
- 简单易懂的图形界面

算法友好

- 支持国密算法测试
- 支持自定义算法

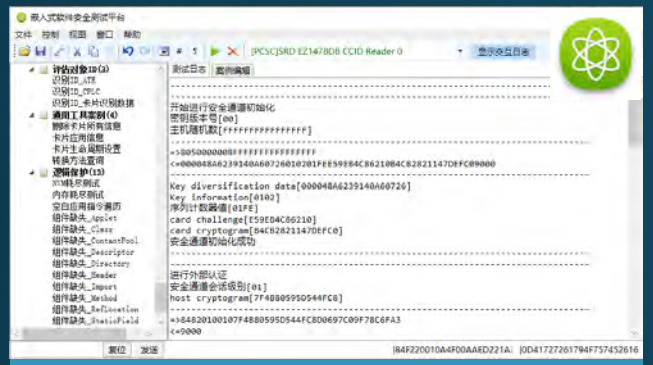
二、错误注入设备

c，设备组件

序号	软件组件	用途说明
1	错误注入软件平台	对硬件系统进行控制，对多种算法进行差分错误分析，推导密钥
2	国密算法包	增加对国密算法SM2，SM4的支持

序号	硬件组件	用途说明
1	激光注入台模块	通过显微镜对芯片发射激光脉冲进行注入攻击
2	电压毛刺注入模块	使用精确的电压毛刺发生电路对被测物进行毛刺攻击
3	电磁注入模块	通过电磁探头对被测物进行高功率的瞬时电磁波注入攻击
4	测试工作站	运行错误注入软件，操作硬件设备及执行测试脚本
5	高级示波器	观察信号波形方便确认攻击位置

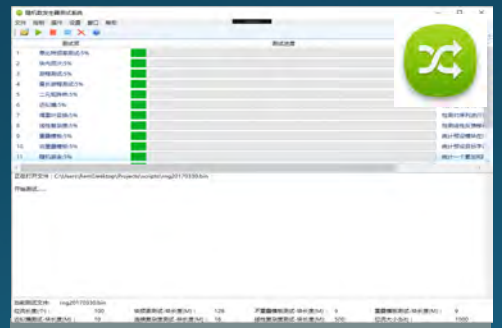
软件测试工具



嵌入式软件测试

APP智云检测平台

密码算法强度测试软件



随机数测试系统

嵌入式软件测试

智能芯片卡上的嵌入式软件和系统的安全测试

密码算法强度测试软件

对密码算法的强度进行明密文独立性检测， 明文扩散性，密钥有效性和密文随机性检测

随机数测试系统

依据国际和中国标准对随机数发生器产生的随机数进行质量测试

APP 智云检测平台

一级-病毒、木马查杀

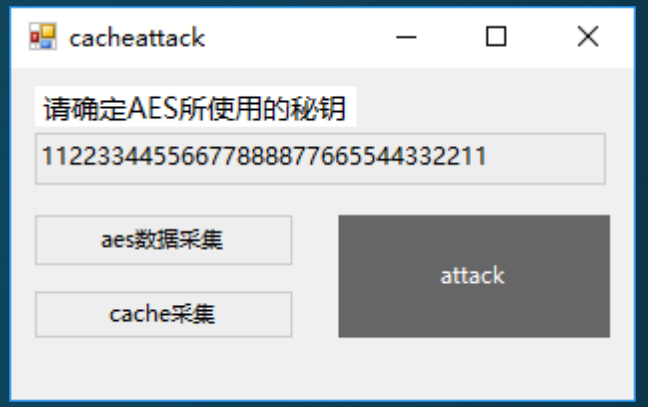
二级-漏洞扫描

三级-风险预警

四级-定制解决方案

软件测试工具

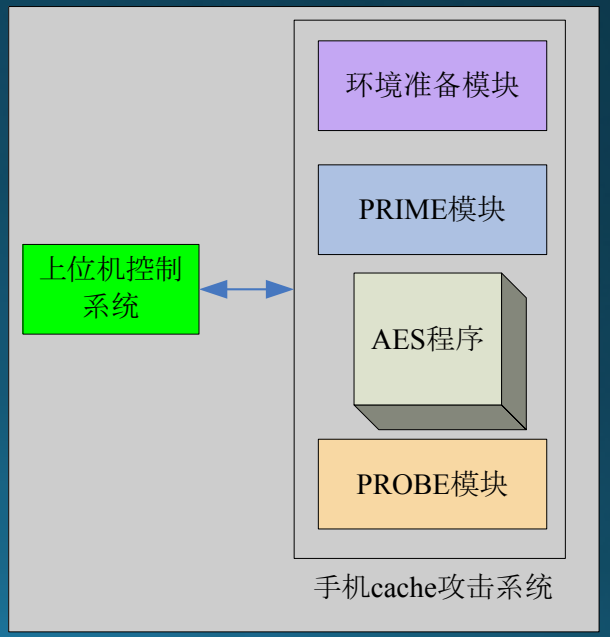
Cache攻击工具



主要功能：
破解手机主处理器中的Cache缓存内容。测试cache是否具有足够的防护。

系统模块：

- 环境准备模块
- Prime模块
- AES程序
- Probe模块



软件测试工具

Cache攻击工具

组件：
上位机软件：CacheAttacker
手机软件： CacheAttackExample

支持环境：

- ARM A53系列架构手机或移动终端
- 手机操作系统：Android
- 上位机操作系统：Windows 10/8

软件测试工具

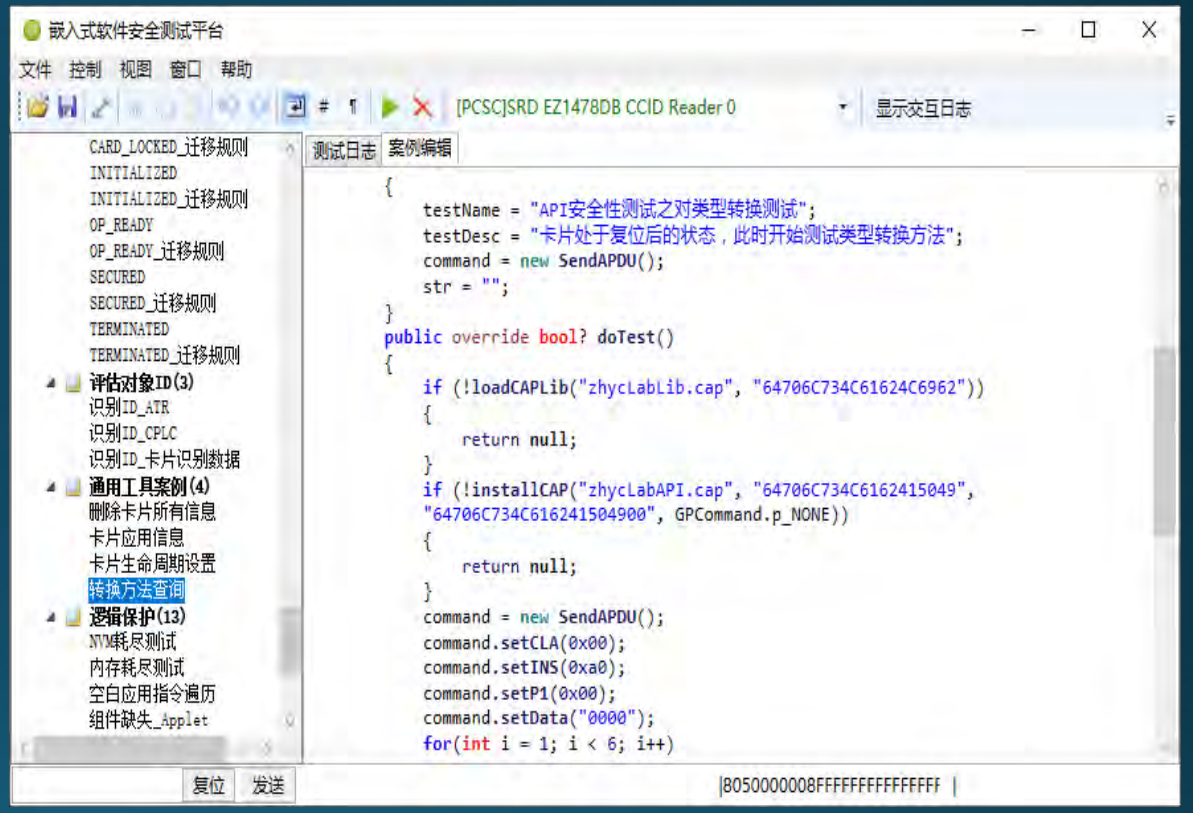
嵌入式软件测试工具

主要功能：
测试SE或IC卡上OS的安全性。可自动化或半自动化对片上OS进行穿透测试和漏洞分析。并可输出详细的测试log供用户解析。

组件：
上位机软件：嵌入式软件测试平台
庞大的测试案例库
通讯硬件：读卡器或开发板

支持环境：

- Java card platform片上OS
- 芯片通讯接口：ISO7816或SWP协议接口
- 上位机操作系统：Windows 10/8



Secure Your Life

谢谢！

安焘
Tel:13811552057
AN@DPLSLAB.com