

纽创信安
Open Security Research

OPEN SECURITY RESEARCH

侧信道 · 故障注入 · 渗透测试

OSR
硬件安全生态

开放实验设备与开源工具链，让硬件安全研究透明可得。

故障注入
电压 · 时钟 · 电磁

侧信道
探测 · 放大 · 滤波

渗透测试
调试 · 总线 · 评估

实验设备 · 开源工具
lab.osr-tech.com



故障注入核心主控 · 电压短路故障注入

故障注入

PowerShorter

本身支持高速电压短路故障注入，并可通过双引擎接口驱动时钟故障与电磁脉冲模块。

电压短路注入
10 ns 双短路引擎
8 段脉冲序列控制

设备上下电
GPIO 与双继电器
设备自动断电复位

Python 驱动
跨平台脚本控制
边沿与计数触发

支持平台：Windows · macOS · Linux

SMA-E1 / E2 双通道脉冲输出

PowerShorter 脉冲输出驱动 · 时钟与电磁故障扩展模块



时钟故障产生器

故障注入

CycleWarper

OLED 屏幕显示 · 频率数字旋钮可调

100 MHz
时钟频率可调上限

1 MHz
最小频率调节步进

由 PowerShorter 驱动，向目标时钟线注入毛刺



EMFI 电磁脉冲产生器

故障注入

EMPulser

快拆探头设计 · 数码显示 · 局部电磁干扰

320 V
脉冲电压可调上限

10–80 ns
窄脉冲输出脉宽范围

由 PowerShorter 驱动，非侵入式局部电磁注入

● 故障注入套件开源 Python 驱动与实验示例

gitee.com/osr-tech/powershorter



侧信道采集探头

侧信道

EMProbe

有源探头设计 · 内置信号放大电路 · 捕捉芯片微弱近场辐射

1 mm
空间采集分辨率

有源放大
内置前端放大电路

高灵敏度近场电磁信号探测，适配各类封装芯片表面扫描



低噪声宽带放大器

侧信道

RF-AMP

宽频带射频信号放大 · 显著提升微弱侧信道泄漏信噪比

30 dB
信号放大增益

9 kHz–6 GHz
工作频率范围

适配侧信道电磁辐射与采样电阻功耗采集链路



高阶低通滤波器 · 50 Ω 阻抗

侧信道

低通滤波器

Low Pass Filter · 滤除高频开关噪声并突出目标密码运算频段

1.2 MHz	4 MHz	7 MHz	20 MHz

提供四种截止频率规格，串联于示波器采集前端



8 位 AVR 硬件安全评估板

侧信道 故障注入

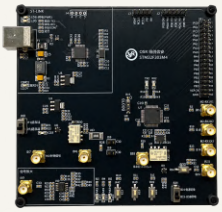
OSR-2560

ATmega2560 · Arduino 兼容 · 功耗采集与电压短路故障注入

算法工程 AES DES SM2 SM3 SM4 RSA

256 KB Flash · 16 MHz · 4 路 SMA 采集口

gitee.com/osr-tech/osr-2560



STM32 硬件安全开发板

侧信道 故障注入

STM32F303M4

STM32F303RCT6 · 板载 ST-LINK · 故障注入与功耗采集

算法工程 AES SM2 SM4 RSA ASCON ML-KEM

256 KB Flash · 32 路 IO · USB / SWD / USART

gitee.com/osr-tech/osr-303



FPGA 硬件安全评估板

侧信道 故障注入

OSR-FPGA-A7100T

XC7A100T-2FGG484C · 功耗采集 · 外部时钟输入

算法工程 AES DES SM2 SM4 ECDSA SM3

16 MB Flash · 50 MHz 晶振 · USB / FT232 / JTAG

gitee.com/osr-tech/osr-fpga-a7100t



6 路 USB 智能集线器

故障注入 侧信道 渗透测试

SmartHub

用于被测 USB 设备自动化上下电与硬复位 · 实时监测各路电压/电流/功率 · 过流保护

6 路独立上下电
上位机脚本控制通断与故障恢复

1 A / 20 W
单路最大电流 / 整机总功率

USB 2.0 · 双 UI 界面切换

gitee.com/osr-tech/osr_smart_hub



多功能硬件接口调试器

渗透测试 故障注入 侧信道

OSR Glasgow

用于驱动 UART / SPI / I²C / JTAG / SWD 等总线通信、输出硬件触发信号及协议交互测试

总线通信 + 输出触发
Python + FPGA 可重构协议与同步触发

1.8–5.0 V / 16 路
自适应电平 · 最高 100 MHz 信号速率

支持读取断电状态、独立限流保护与自定义硬件协议脚本扩展



开源硬件 USB 2.0 协议分析仪

渗透测试

USBTrace T1

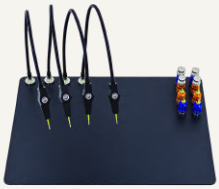
非侵入式硬件监听 · 自定义触发信号输出 · 配套自研包解析图形界面程序

480 Mbps
高速 / 全速 / 低速捕获

32 MB
板载高速缓存 SDRAM

自研包解析界面与总线触发

gitee.com/osr-tech/usb-trace-t1



柔性探针台

侧信道 故障注入 渗透测试

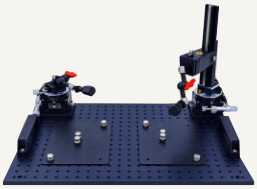
FlexHolder

可调金属万向探臂 · 磁吸固定卡具 · 适用于 PCB 信号点位探测与探头稳固夹持

万向柔性
多自由度探臂调节

磁吸底座
电路板快速夹具固定

支持多探针协同固定、测试点快速压接与近场探头悬停



高精度位移实验台

侧信道 故障注入

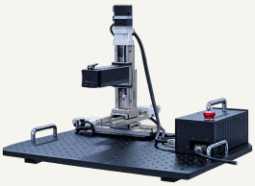
手动三轴平台

6061-T6 铝合金阳极氧化 · 快拆底盘设计 · 360° 蛇形夹持臂精准对准芯片表面

±12.5 mm
XY 轴微调行程

0.03 mm
千分尺定位精度

支持多路位移台并行架设，适配 EMProbe 与 EMPulser 定点实验



开放式精密定位平台

侧信道 故障注入

电动三轴平台

Python 脚本与摇杆双模控制 · 物理与软件双重限位 · 集成急停开关 · 支持芯片全表面网格扫描

100 mm
最大物理行程（限位 80 mm）

±0.5 μm
重复定位精度（单向 10 μm）

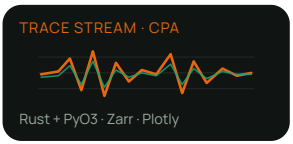
自动化芯片表面扫描与敏感点测绘

gitee.com/osr-tech/nuxyz

NUSCAR 侧信道

高性能侧信道分析工具箱

贯通曲线采集、信号处理、分析与可视化，为硬件安全研究与密码教学提供全流程开源软件支持。

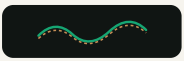


统一分析工作流

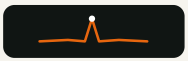
ACQUIRE → PROCESS → ANALYZE → VISUALIZE



曲线采集
Scope / Communicator



信号处理
滤波 · 对齐 · 重采样



侧信道分析
分析 · 评估 · 建模



结果可视化
曲线 · 热力图 · 频谱

高性能与扩展

Rust + PyO3 核心加速
Python API · 并行计算
支持自定义扩展分析方法

分析与评估

CPA / DPA / LRA / MIA
TTest / ANOVA / NICV / SNR
模板分析 · 机器学习建模

处理与算法模型

滤波 / 对齐 / PCA / 重采样
AES / DES / SM4 / HMAC
支持高阶组合分析

曲线管理与可视化

Zarr / ETS / TRS / H5 / NPY
Plotly 交互图形 · 自动降采样
曲线 / 热力图 / 频谱图

数据集与教学资源

开源社区仓库

涵盖 DPA · ASCAD · CHES CTF · EdDSA · Dilithium 数据集，配套 Jupyter Notebook 示例与视频教程。

gitee.com/osr-tech/nuscar

学习科研使用 · 商业产品集成需获取商业许可

扫码访问项目与教程

纽创信安
Open Security Research

OPEN SECURITY RESEARCH

共建开放的硬件安全生态

让硬件安全研究透明可得

实验室官网

B站视频

Gitee 开源

淘宝店铺

sales@osr-tech.com

lab.osr-tech.com

深圳：深圳市南山区粤海街道高新区社区深圳湾科技生态园二区9栋503-506

北京：北京市海淀区东北旺西路中关村软件园一期17号楼高科岭A205